Rouse and Zureick-Brown *Research in Number Theory*
DOI 10.1007/s40993-015-0013-7

Research in Number Theory
a SpringerOpen Journal

RESEARCH ARTICLE Open Access

Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois

Jeremy Rouse[1] and David Zureick-Brown[2*]

*Correspondence:
dzb@mathcs.emory.edu
[2]David Zureick-Brown, Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322 USA
Full list of author information is available at the end of the article

Abstract

We give a classification of all possible 2-adic images of Galois representations associated to elliptic curves over $\mathbb{Q}$. To this end, we compute the 'arithmetically maximal' tower of 2-power level modular curves, develop techniques to compute their equations, and classify the rational points on these curves.

1 Introduction

Serre proved in [39] that, for an elliptic curve E over a number field K without complex multiplication, the index of the mod n Galois representation $\rho_{E,n}$ associated to E is *bounded* – there is an integer N_E such that for any n, the index of $\rho_{E,n}(G_K)$ in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is at most N_E (equivalently, the mod ℓ representation is surjective for large ℓ). Serre's proof is ineffective in the sense that it does not compute N_E explicitly; in fact one conjectures that for $\ell > 37$, $\rho_{E,\ell}$ is surjective. The early progress on this problem [31] has recently been vastly extended [6], but a proof in the remaining case – to show that the image cannot be contained in the normalizer of a non-split Cartan – is elusive and inaccessible through refinements of Mazur's method.

Mazur's Program B [30] (given an open subgroup $H \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$, classify all elliptic curves E/K such that the image of $\rho_E = \varprojlim_n \rho_{E,n}$ is contained in H) suggests a more general uniformity conjecture – one expects that for every number field K, there exists a constant $B(K)$ such that for every elliptic curve E/K without complex multiplication, the *index* of $\rho_E(G_K)$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is bounded by $B(K)$.

Computational evidence supports the uniformity conjecture – for any given E, [54] gives an algorithm (implemented in Sage) to compute the set of primes ℓ such that $\rho_{E,\ell}$ is not surjective, and verifies for non-CM E with $N_E \leq 350000$ that $\rho_{E,\ell}$ is surjective for $\ell > 37$. Similarly, for small ℓ one can compute $\mathrm{im}\rho_{E,\ell}$ directly; [48] has computed $\mathrm{im}\rho_{E,\ell}$ for every elliptic curve in the Cremona and Stein-Watkins databases for all primes $\ell < 80$. This is a total of 139 million curves, and Sutherland's results are now listed in Cremona's tables. In Appendix A, we describe a method using [17] that can often provably compute the mod n image of Galois for any elliptic curve.

Complementing this are various results (going as far back as Fricke, possibly earlier; see ([30], Footnote 1)) computing equations for the modular curve X_H parameterizing E with $\rho_E(G_K) \subset H$ (see Section 2 for a definition). For instance, [5] have extended the range of ℓ such that one can compute the modular polynomial $\Phi_\ell(X, Y)$ to $\ell \approx 10{,}000$

and Sutherland now maintains tables of equations for modular curves (see e.g. [47, 49]). Recently [16] (inspired by the earlier 3-adic analogue [20]) computed equations for the modular curves necessary to compute whether the mod 8, and thus the 2-adic, image of Galois is surjective (i.e. equations for X_H with reduction $H(8) \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ a maximal subgroup). (See Remark 4.1 for more such examples.)

In many cases these equations have been used to compute the rational points on the corresponding curves; see Remark 4.1 for some examples. Applications abound. In addition to verifying low level cases of known classification theorems such as [31] (in this spirit we note the outstanding case of the "cursed" genus 3 curve $X_{ns}^+(13)$ ([4, 6], Remark 4.10)) and verifying special cases of the uniformity problem, various authors have used the link between integral points on modular curves and the class number one problem to give new solutions to the class number one problem; see ([40], A.5), and more recently [2, 3, 13, 28, 45].

1.1 Main theorem

In the spirit of Mazur's 'Program B', we consider a "vertical" variant of the uniformity problem. For any prime ℓ and number field K, it follows from Falting's Theorem and a short argument (e.g. [1], Theorem 1.2, plus Goursats Lemma) that there is a bound $N_{\ell,K}$ on the index of the image of the ℓ-adic representation associated to any elliptic curve over K. The uniformity conjecture implies that for $\ell > 37$, $N_{\ell,\mathbb{Q}} = 1$, but N_ℓ can of course be larger for $\ell \leq 37$. Actually even more is true – the uniformity conjecture would imply the existence of a universal constant N bounding the index of $\rho_{E,n}(G_\mathbb{Q})$ for every n (equivalently, bounding the index of $\rho_E(G_\mathbb{Q})$; see [1]).

In this spirit, we give a complete classification of the possible 2-adic images of Galois representations associated to non-CM elliptic curves over $\mathbb{Q}$ and, in particular, compute $N_{2,\mathbb{Q}}$.

Theorem 1.1. *Let $H \subseteq GL_2(\mathbb{Z}_2)$ be a subgroup, and E be an elliptic curve whose 2-adic image is contained in H. Then one of the following holds:*

- *The modular curve X_H has infinitely many rational points.*
- *The curve E has complex multiplication.*
- *The j-invariant of E appears in the following Table 1 below.*

Remark 1.2. The level of a subgroup H is the smallest integer 2^k so that H contains all matrices $M \equiv I \pmod{2^k}$. Also, we consider action of the matrices in $\mathrm{GL}_2(\mathbb{Z}_2)$ on the *right*. That is, we represent elements of $E[2^k]$ as row vectors $\vec{x}$, and the image of Galois on an element of $E[2^k]$ corresponds to $\vec{x}M$.

Corollary 1.3. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Then the index of $\rho_{E,2^\infty}(G_\mathbb{Q})$ divides 64 or 96; all such indices occur. Moreover, the image of $\rho_{E,2^\infty}(G_\mathbb{Q})$ is the inverse image in $GL_2(\mathbb{Z}_2)$ of the image of $\rho_{E,32}(G_\mathbb{Q})$. For non-CM elliptic curves $E/\mathbb{Q}$, there are precisely 1208 possible images for $\rho_{E,2^\infty}$.*

Remark 1.4. The earlier paper [35] of Nishioka studied the case of an elliptic curve $E/\mathbb{Q}$ with full rational 2-torsion. Nishioka proved that $\rho_{E,2^\infty}(G)$ contains

Table 1 Exceptional j-invariants from Theorem 1.1

j-invariant	level of H	Generators of image
2^{11}	16	$\begin{bmatrix} 7 & 14 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 5 \\ 6 & 11 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 7 \end{bmatrix}$
$2^4 \cdot 17^3$	16	$\begin{bmatrix} 7 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 5 \\ 14 & 7 \end{bmatrix}, \begin{bmatrix} 7 & 7 \\ 2 & 1 \end{bmatrix}$
$\frac{4097^3}{2^4}$	16	$\begin{bmatrix} 3 & 5 \\ 6 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 5 \\ 14 & 7 \end{bmatrix}, \begin{bmatrix} 7 & 7 \\ 2 & 1 \end{bmatrix}$
$\frac{257^3}{2^8}$	16	$\begin{bmatrix} 7 & 14 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 5 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 5 \\ 6 & 3 \end{bmatrix}$
$-\frac{857985^3}{62^8}$	32	$\begin{bmatrix} 25 & 18 \\ 2 & 7 \end{bmatrix}, \begin{bmatrix} 25 & 25 \\ 2 & 7 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 8 & 1 \end{bmatrix}, \begin{bmatrix} 25 & 11 \\ 2 & 7 \end{bmatrix}$
$\frac{919425^3}{496^4}$	32	$\begin{bmatrix} 29 & 0 \\ 4 & 1 \end{bmatrix}, \begin{bmatrix} 31 & 27 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 31 & 31 \\ 2 & 1 \end{bmatrix}$
$-\frac{3 \cdot 18249920^3}{17^{16}}$	16	$\begin{bmatrix} 4 & 7 \\ 15 & 12 \end{bmatrix}, \begin{bmatrix} 7 & 14 \\ 7 & 9 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 11 & 9 \end{bmatrix}$
$-\frac{7 \cdot 1723187806080^3}{79^{16}}$	16	$\begin{bmatrix} 4 & 7 \\ 15 & 12 \end{bmatrix}, \begin{bmatrix} 7 & 14 \\ 7 & 9 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 11 & 9 \end{bmatrix}$

the kernel of reduction modulo 128, and also that if E has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, then $\rho_{E,2^\infty}(G)$ is conjugate to $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}_2) : a \equiv 1 \pmod 8, \right.$ $\left. b \equiv 0 \pmod 2, c \equiv 0 \pmod 8 \text{and } d \equiv 1 \pmod 2 \right\}$.

Remark 1.5. All indices dividing 96 occur for infinitely many elliptic curves. For the first six j-invariants in the table above, the index of the image is 96, and for these, $-I \in H$ and this index occurs for all quadratic twists. Additionally, there are several subgroups H with $-I \notin H$ and $X_H \cong \mathbb{P}^1$, so that the there are infinitely many j-invariants such that the index is 96. Index 64 only occurs for the last two j-invariants in the above table, which occur as the two non-cuspidal non-CM rational points on the genus 2 curve $X_{ns}^+(16)$ (X_{441} on our list; see the analysis of Subsection 8.3), which classifies E whose mod 16 image is contained in the normalizer of a non-split Cartan. (The second j-invariant was missed in [3], because the map from $X_{ns}^+(16)$ to the j-line was not correctly computed. In this computation, Baran relied on earlier computations of Heegner, and the error could be due to either of them.) The smallest conductor of an elliptic curve with this second j-invariant is $7^2 \cdot 79 \cdot 106123^2$ (which is greater than $4 \cdot 10^{13}$).

Remark 1.6. An application of the classification is an answer to the following question of Stevenhagen: when can one have $\mathbb{Q}(E[\,2^{n+1}]\,) = \mathbb{Q}(E[\,2^n]\,)$ for a non-CM curve E? The answer is that if $n > 1$, $\mathbb{Q}(E[\,2^{n+1}]\,)$ is larger than $\mathbb{Q}(E[\,2^n]\,)$. On the other hand, there is a one-parameter family of curves for which $\mathbb{Q}(E[\,2]\,) = \mathbb{Q}(E[\,4]\,)$. These are parametrized by the modular curve X_{20b}, and one example is the curve $E : y^2 + xy + y = x^3 - x^2 + 4x - 1$.

Remark 1.7. The classification above plays a role in González-Jiménez and Lozano-Robledo's classification of all cases in which $\mathbb{Q}(E[\,n]\,)/\mathbb{Q}$ is an abelian extension of $\mathbb{Q}$. See [23].

Remark 1.8. A surprising fact is that not every subgroup H such that $X_H(\mathbb{Q})$ is infinite occurs as the image of Galois of an elliptic curve over $\mathbb{Q}$; see Section 6.

Remark 1.9. In preparation by other authors is a related result (Sutherland, A, Zywina, D: Modular curves of genus zero and prime-power level, in preparation) – for every subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}_\ell)$ such that $-I \in H$, $\det(H) = \widehat{\mathbb{Z}}^\times$, and X_H has genus 0, they compute equations for X_H, whether $X_H(\mathbb{Q}) = \emptyset$ and, if not, equations for the map $X_H \to X(1)$.

Remark 1.10. The image of the 2-adic representation is connected with the following problem in arithmetic dynamics. Given an elliptic $E/\mathbb{Q}$ and a point $\alpha \in E(\mathbb{Q})$ of infinite order, what is the density of primes p for which the order of the reduction $\tilde{\alpha} \in E(\mathbb{F}_p)$ is odd?

In [27], Rafe Jones and the first author study this question, and show (see [27, Theorem 3.8]) that if for each n, β_n is a chosen preimage of α with $2^n\beta_n = \alpha$ and the fields $\mathbb{Q}(\beta_n)$ and $\mathbb{Q}(E[2^n])$ are linearly disjoint for all n, then this density is given by

$$\int_{\mathrm{im}\rho_{E,2^\infty}} |\det(M - I)|_\ell \, d\mu,$$

an integral over the 2-adic image. In the case that $\rho_{E,2^\infty}$ is surjective, this density equals $\frac{11}{21} \approx 0.5238$. Our calculations show that for a non-CM elliptic curve E, this generic density can be as large as $\frac{121}{168} \approx 0.7202$ (corresponding to elliptic curves with no rational 2-torsion, square discriminant, whose mod 4 image does not contain $-I$, namely curves parametrized by X_{2a}), and as small as $\frac{1}{28} \approx 0.0357$ which is attained for several 2-adic images, including elliptic curves whose torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. The generic density is listed on the summary page for each subgroup.

We now give a brief outline of the proof of Theorem 1.1. For a subgroup H of $\mathrm{GL}_2(\mathbb{Z}_2)$ of finite index, there is some k such that $\Gamma(2^k) \subset H$. The non-cuspidal points of the modular curve $X_H := X(2^k)/H$ then roughly classify elliptic curves whose 2-adic image of Galois is contained in H; see Section 2 for a more precise definition.

The idea of this paper is to find all of the rational points on the "tower" of 2-power level modular curves (see Fig. 1). We only consider subgroups H such that H has surjective determinant and contains an element with determinant -1 and trace zero (these conditions are necessary for $X_H(\mathbb{Q})$ to be non-empty). In our proof, we will handle the case $-I \in H$ first; see Subsection 2.1 for a discussion of X_H and the distinction between the cases $-I \in H$ and $-I \notin H$.

Proof of Theorem 1.1. The proof naturally breaks into the following steps.

(1) (Section 3.) First we compute a collection $\mathcal{C}$ of open subgroups $H \subset \mathrm{GL}_2(\mathbb{Z}_2)$ such that every open $K \subset \mathrm{GL}_2(\mathbb{Z}_2)$ which satisfies the above necessary conditions and which is not in $\mathcal{C}$ is contained in some $H \in \mathcal{C}$ such that $X_H(\mathbb{Q})$ is finite. (See Fig. 1 for those with $-I \in H$.)

(2) (Section 4.) Next, we compute, for each $H \in \mathcal{C}$ equations for (the coarse space of) X_H and, for any K such that $H \subset K$, the corresponding map $X_H \to X_K$.

(3) (Section 5.) Then, for $H \in \mathcal{C}$ such that $-I \notin H$ we compute equations for the universal curve $E \to U$, where $U \subset X_H$ is the locus of points with $j \neq 0, 1728$ or ∞.

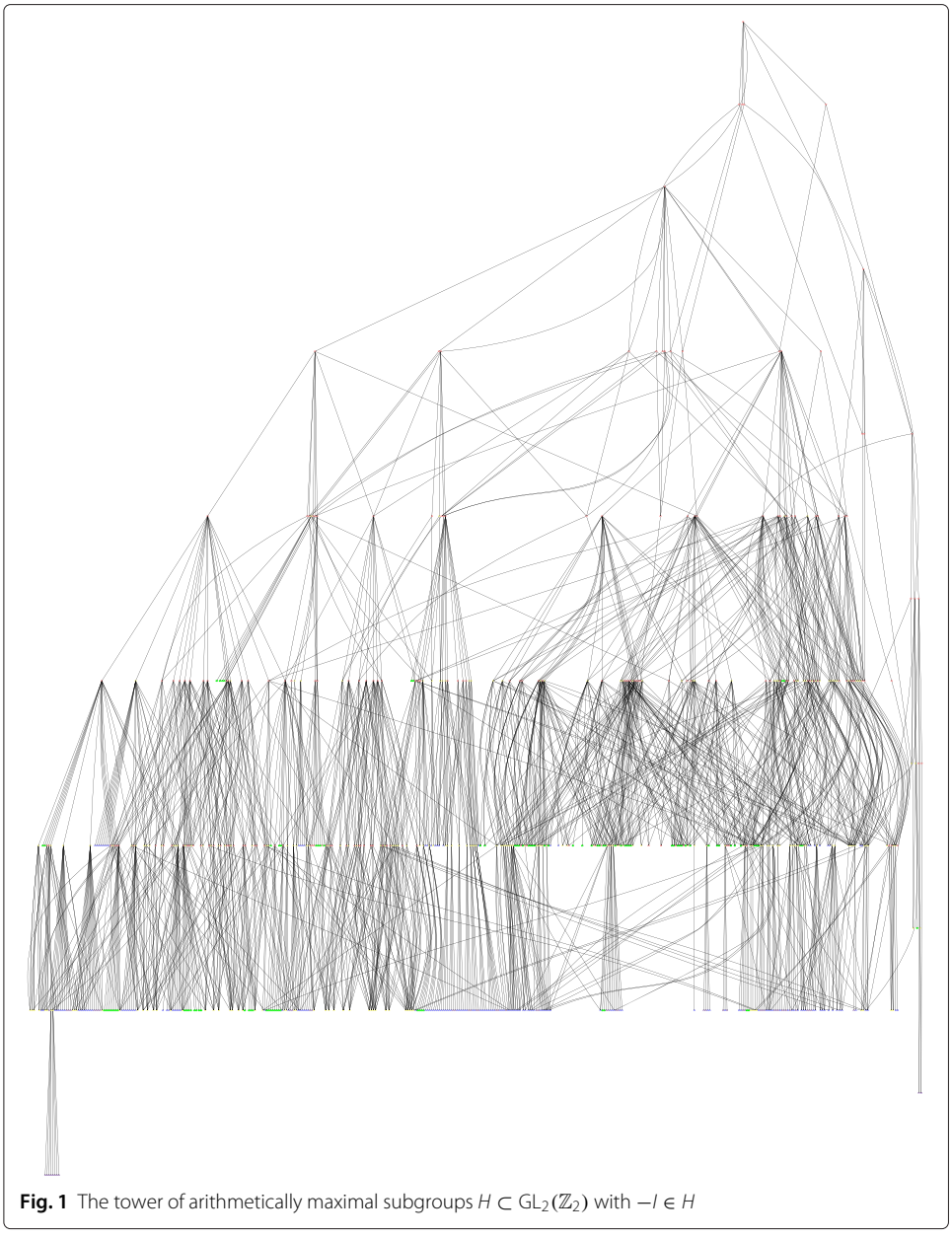


Fig. 1 The tower of arithmetically maximal subgroups $H \subset \mathrm{GL}_2(\mathbb{Z}_2)$ with $-I \in H$

(4) (Remainder of paper.) Finally, with the equations in hand, we determine $X_H(\mathbb{Q})$ for each $H \in \mathcal{C}$. The genus of X_H can be as large as 7.

(5) (Appendix.) If we find a non-cuspidal, non-CM rational point on a curve X_H with genus ≥ 2, we use computations of resolvent polynomials (as described in [17]) to prove that the 2-adic image for the corresponding elliptic curve E is H.

Remark 1.11. (Étale descent via group theory) The analysis of rational points on the collection of X_H involves a variety of techniques, including local methods, Chabauty and elliptic curve Chabauty, and étale descent.

To determine the rational points on some of the genus 5 and 7 curves we invoke a particularly novel (and to our knowledge new) argument, combining étale descent with

group theory. In short, some of the X_H admit an étale double cover $Y \to X_H$ such that Y is isomorphic to $X_{H'}$ for some subgroup H' of H. More coincidentally, each of the twists Y_d relevant to the étale descent are *also* isomorphic to modular curves $X_{H'_d}$ for some group H'_d. And finally, each group H'_d is a subgroup of some additional larger group H''_d such that $X_{H''_d}$ is a curve with finitely many rational points we already understand (e.g. a rank 0 elliptic curve), and the map $X_{H'_d} \to X_{H''_d}$ determines $X_{H'_d}(\mathbb{Q})$ and thus, by étale descent $X_H(\mathbb{Q})$. This method is applicable to 20 out of the 24 curves of genus greater than 3 that we must consider. See Subsection 7.4.

2 The modular curves X_H

Given a basis (P_1, P_2) of $E(\overline{\mathbb{Q}})[N]$ we identify $\psi\colon (\mathbb{Z}/N\mathbb{Z})^2 \cong E(\overline{\mathbb{Q}})[N]$ via the map $\psi(e_i) = P_i$. This gives rise to *two* isomorphisms $\iota_1, \iota_2\colon \mathrm{Aut}\, E(\overline{\mathbb{Q}})[N] \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (corresponding to a choice of left vs right actions) as follows: if $\phi \in \mathrm{Aut}\, E(\overline{\mathbb{Q}})[N]$ satisfies

$$\begin{aligned}\phi(P_1) &= aP_1 + cP_2\\ \phi(P_2) &= bP_1 + dP_2,\end{aligned}$$

then we define

$$\iota_1(\phi) := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } \iota_2(\phi) := \begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

These correspond respectively to left (via column vectors) and right (via row vectors) actions of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $(\mathbb{Z}/N\mathbb{Z})^2$. Alternatively, $\iota_i(\phi)$ is defined by commutativity of the diagram

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^2 & \xrightarrow{\psi} & E[N] \\ {\scriptstyle \iota_i(\phi)}\downarrow & & \downarrow{\scriptstyle \phi} \\ (\mathbb{Z}/N\mathbb{Z})^2 & \xrightarrow[\psi]{} & E[N] \end{array}$$

where we consider $\iota_i(\phi)$ acting on the left (via column vectors) for $i = 1$ and on the right (via row vectors) for $i = 2$.

Throughout this paper we use only right actions, and in particular define $\rho_{E,N}\colon G_K \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as $\rho_{E,N}(\sigma) := \iota_2(\sigma)$ (this is consistent with, for instance, [41]). Many sources are ambiguous about this choice, but the ambiguity usually does not matter (see Remark 2.2).

For an integer N, we define the modular curve $Y(N)/\mathbb{Q}$ to be the moduli space parameterizing pairs $(E/S, \iota)$, where E is an elliptic curve over some base scheme $S/\mathbb{Q}$ and ι is an isomorphism $M_S := (\mathbb{Z}/N\mathbb{Z})^2_S \cong E[N]$, and define $X(N)$ to be its smooth compactification (see ([18], II) for a modular interpretation of the cusps). Note that $X(N)$ is not geometrically connected (and thus differs from the geometrically connected variant of ([30], Section 2) where ι is "canonical" in that it respects the Weil pairing), and that a matrix $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $X(N)$ (on the right) via precomposition with

$$M \xrightarrow{A} M,\ \vec{v} \mapsto \vec{v}A$$

so that $A \cdot (E, \iota) := (E, \iota \circ A)$.

Following [18], for a subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ and an integer N such that H contains the kernel of the reduction map $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we define X_H to be the quotient of

the modular curve $X(N)$ by the image $H(N)$ of H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. This quotient is independent of N, is geometrically connected if $\det(H) = \widehat{\mathbb{Z}}^\times$, and roughly classifies elliptic curves whose adelic image of Galois is contained in H. By the definition of X_H as a quotient, the non-cuspidal K-rational points of X_H correspond to G_K-stable H-orbits of pairs (E, ι); we make the translation to the image of Galois more precise in the following lemma.

Lemma 2.1. *Let E be an elliptic curve over a number field K. Then there exists an ι such that $(E, \iota) \in X_H(K)$ if and only if $\mathrm{im}\rho_{E,n}$ is contained in a subgroup conjugate to H.*

Proof. For $\sigma \in G_K$ and $(E, \iota) \in X_H(K)$, ι^σ is defined to be the composition $M_K \xrightarrow{\iota} E[N] \xrightarrow{\sigma} E[N]$. If $(E, \iota) \in X_H(K)$, then for every $\sigma \in G_K$, there is some $A \in H$ such that $\iota^\sigma = \iota \circ A$. Set $P_i := \iota(e_i)$ and suppose that $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$. Then

$$(\iota \circ A)(e_1) = \iota(e_1 A) = \iota(ae_1 + ce_2) = aP_1 + cP_2 = P_1^\sigma$$
$$(\iota \circ A)(e_2) = \iota(e_2 A) = \iota(be_1 + de_2) = bP_1 + dP_2 = P_2^\sigma,$$

so $\rho_{E,N}(\sigma) = A$ and $\mathrm{im}\rho_{E,N} \subset H$ as claimed.

Conversely, let P_1, P_2 be a basis of $E(\overline{K})[N]$ such that $\mathrm{im}\rho_{E,N} \subset H$ with respect to this basis, and define ι by $\iota(e_i) := P_i$. For $\sigma \in G_K$, $\rho_{E,N}(\sigma) = A$ where

$$A := \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

and

$$P_1^\sigma := aP_1 + cP_2$$
$$P_2^\sigma := bP_1 + dP_2.$$

By assumption, $A \in H$; moreover

$$\iota^\sigma(e_1) = \iota(ae_1 + ce_2) = aP_1 + cP_2$$
$$\iota^\sigma(e_2) = \iota(be_1 + de_2) = bP_1 + dP_2$$

and so $\iota^\sigma = \iota \circ A$, which proves the converse. □

Remark 2.2. As discussed above, a choice of basis for $E[N]$ gives rise to *two* isomorphisms $\iota_1, \iota_2 \colon \mathrm{Aut}\, E[N] \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, via column and row vectors. Given $K \subset \mathrm{Aut}\, E[N]$, the images $\iota_i(K)$ generally differ; in fact, $\iota_1(K) = \iota_2(K)^T$, where we define the *transpose* $H^T := \{A^T : A \in H\}$. In the literature the choice of left or right action is often ambiguous, but usually does not matter: for many common H (e.g. the normalizer of a Cartan subgroup) H is conjugate to H^T and the modular curves X_H and X_{H^T} are thus isomorphic. This is an issue in this paper; if instead we use ι_1, then X_H parametrizes E with image contained in H^T rather than H, and in general H^T and H are not conjugate.

In general X_H is a stack, and if $-I \in H$, then the stabilizer of every point contains $\mathbb{Z}/2\mathbb{Z}$. (Some, but not all, of the CM points with $j = 0$ or 12^3 will have larger stabilizers.) In contrast, when $-I \notin H$, X_H no longer has a generic stabilizer, but is generally still a stack since the CM points may have stabilizers. When $-I \in H$, quadratic twisting preserves the

property that $\mathrm{im}\rho_{E,N} \subset H$; in contrast, when $-I \notin H$, given a non-CM elliptic curve E/K such that $j(E)$ is in the image of the map $j\colon X_H(K) \to \mathbb{P}^1(K)$, there is a unique quadratic twist E_d of E such that $\mathrm{im}\rho_{E,N} \subset H$ (see Lemma 5.1 below).

There exists a coarse space morphism, i.e. a morphism $\pi\colon X_H \to X$, where X is a scheme, such the map $X_H(\overline{\mathbb{Q}}) \to X(\overline{\mathbb{Q}})$ is a bijection, and any map from X_H to a scheme uniquely factors through this morphism. We compute equations for the coarse space of X_H (and with no confusion will use the same notation X_H for the coarse space). The coarse space has the following moduli interpretation – given a number field K and a K-point t of the coarse space, there exists an elliptic curve with j-invariant $j(t)$ (where j is the map $X \to X(1)$) satisfying $\mathrm{im}\rho_{E,N} \subset H$, and conversely, for any E/K such that $\mathrm{im}\rho_{E,n} \subset H$, there exists a K-point t of the coarse space of X_H such that $j(t) = j(E)$.

For more details see ([18], IV-3); alternatively, for a shorter discussion see ([3], Section 3), ([40], A.5) or ([30], Section 2).

2.1 Universal curves

Suppose that $-I \notin H$. Since we are not interested in the CM points anyway, we consider the complement $U \subset X_H$ of the cusps and preimages on X_H of $j = 0$ and $j = 1728$. Then U is a scheme, so there exists a universal curve $\mathscr{E} \to U$; i.e. a surface $\mathscr{E}$ with a map $\mathscr{E} \to U$ such that for every $t \in U(K)$, the fiber $\mathcal{E}_t$ is an elliptic curve over K without CM such that $\mathrm{im}\rho_{E,n} \subset H$, and conversely for any elliptic curve E over a field K such that $\mathrm{im}\rho_{E,n} \subset H$ there exists a (non-unique) $t \in U(K)$ such that the $E \cong \mathcal{E}_t$.

In preparation for Section 5 (where we compute equations for $\mathscr{E} \to U$), we prove a preliminary lemma on the shape of the defining equations of $\mathscr{E}$.

Lemma 2.4. *Let $f\colon \mathscr{E} \to U$ be as above and assume that $U \subset \mathbb{A}^1$. Then there exists a closed immersion $\mathscr{E} \hookrightarrow \mathbb{P}^2_U$ given by a homogeneous polynomial*

$$Y^2Z - X^3 - aXZ^2 - bZ^3$$

where $a, b \in \mathbb{Z}[t]$.

Proof. The identity section $e\colon U \to \mathscr{E}$ is a closed immersion whose image $e(U)$ is thus a divisor on $\mathscr{E}$ isomorphic to U. By Riemann-Roch, the fibers of the pushforward $f_*\mathcal{O}(3e(U))$ are all 3-dimensional, so by the theorem on cohomology and base change $f_*\mathcal{O}(3e(U))$ is a rank 3 vector bundle on U. Since $U \subset \mathbb{A}^1$, U has no non-trivial vector bundles and so $f_*\mathcal{O}(3e(U))$ is trivial. Let $\mathcal{O}_U^{\oplus 3} \cong f_*\mathcal{O}(3e(U))$ be a trivialization given by sections $1, x, y$, where 1 is the constant section 1 (given by adjunction), x has order 2 along $e(U)$, and y has order 3. These sections determine a surjection $f^*f_*\mathcal{O}(3e(U)) \to \mathcal{O}(3e(U))$ and thus a morphism $\mathcal{E} \to \mathbb{P}^2_U$ which, since the fibers over U are closed immersions, is also a closed immersion; $1, x, y$ satisfy a cubic equation (this is true over the generic point, so true globally) and, since we are working in characteristic 0, can be simplified to short Weierstrass form as desired. □

3 Subgroups of $\mathbf{GL_2}(\mathbb{Z}_2)$

Definition 3.1. Define a subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}_2)$ to be arithmetically maximal if

(1) $\det\colon H \to \mathbb{Z}_2^\times$ is surjective,

(2) there is an $M \in H$ with determinant -1 and trace zero, and
(3) there is no subgroup K satisfying (1) and (2) with $H \subseteq K$ so that X_K has genus ≥ 2.

If $E/\mathbb{Q}$ is an elliptic curve and $H = \rho_{E,2^\infty}(G_\mathbb{Q})$, then the properties of the Weil pairing prove that $\det\colon H \to \mathbb{Z}_2^\times$ is surjective. Also, the image of complex conjugation in H must be a matrix M with $M^2 = I$ and $\det(M) = -1$. This implies that the trace of M equals zero.

Remark 3.2. After the subgroup and model computations were complete, David Zywina and Andrew Sutherland pointed out that if $E/\mathbb{Q}$ is an elliptic curve, complex conjugation fixes an element of $E[n]$. This gives further conditions on a matrix M that could be the image of complex conjugation, and rules out a handful of other subgroups.

We enumerate all of the arithmetically maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ by initializing a queue containing only $H = \mathrm{GL}_2(\mathbb{Z}_2)$. We then remove a subgroup H from the queue, compute all of the open maximal subgroups $M \subseteq H$. We add M to our list of potential subgroups if (i) $\det\colon M \to \mathbb{Z}_2^\times$ is surjective, (ii) $-I \in M$, (iii) M contains a matrix with determinant -1 and trace zero, and (iv) if M is not conjugate in $\mathrm{GL}_2(\mathbb{Z}_2)$ to a subgroup already in our list. If the genus of X_M is zero or one, we also add M to the queue. We proceed until the queue is empty.

To enumerate the maximal subgroups, we use the following results. Recall that if G is a profinite group, then $\Phi(G)$, the Frattini subgroup of G, is the intersection of all open maximal subgroups of G. Proposition 2.5.1(c) of [53] states that if $K \trianglelefteq G$, $H \subseteq G$ and $K \subseteq \Phi(H)$, then $K \subseteq \Phi(G)$. Applying this with $H = N \trianglelefteq G$ and $K = \Phi(N)$, we see that $\Phi(N) \subseteq \Phi(G)$.

Lemma 3.3. *Suppose that* $\Gamma(2^k) \subseteq H \subseteq G$ *and* $k \geq 2$. *If* K *is a maximal subgroup of* H, *then* $\Gamma\left(2^{k+1}\right) \subseteq K$.

Proof. We have that $\Gamma(2^k) \trianglelefteq H$ and by the above argument, we have

$$\Phi(\Gamma(2^k)) \subseteq \Phi(H).$$

Now, $\Gamma(2^k)$ is a pro-2 group and this implies that every open maximal subgroup of $\Gamma(2^k)$ has index 2. Hence,

$$\Phi(\Gamma(2^k)) \supseteq \Gamma(2^k)^2.$$

If $g \in \Gamma(2^k)$, $g = I + 2^k M$ for some $M \in M_2(\mathbb{Z}_2)$. Then,

$$g^2 = I + 2^{k+1}M + 2^{2k}M^2 \equiv I + 2^{k+1}M \pmod{2^{k+2}}$$

provided $k \geq 2$. Hence, the squaring map gives a surjective homomorphism $\Gamma(2^k)/\Gamma(2^{k+1}) \to \Gamma(2^{k+1})/\Gamma(2^{k+2})$ for all $k \geq 2$. It follows that an element in $\Gamma(2^{k+1})$ can be written as a product of squares in every quotient $\Gamma(2^k)/\Gamma(2^{n+k})$ and since the $\Gamma(2^{n+k})$ form a base for the open neighborhoods of the identity in G, we have that $\Gamma(2^{k+1}) \subseteq \Phi(\Gamma(2^k))$. This yields the desired result. □

The enumeration of the subgroups is accomplished using Magma. The initial enumeration produces 1619 conjugacy classes of subgroups. The computation of the lattice of such subgroups finds that many of these are contained in subgroups H where the genus of X_H is ≥ 2. These are then removed, resulting in 727 arithmetically maximal subgroups. The arithmetically maximal subgroups can have genus as large as 7 and index as large as 192.

4 Computing equations for X_H with $-I \in H$

Here we discuss the computation of equations for X_H as H ranges over the arithmetically maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$.

Remark 4.1. Equations for some of these curves already appear in the literature; see [22, 25, 47, 49], ([29], Table 12.1), [16, 42], ([33] Proof of Lemma 3.2), [3, 25, 32, 54]*3.2 for equations of $X_0(N)$ for $N = 2, 4, 8, 16, 32, 64$, $X_1(N)$ for $N = 2, 4, 8, 16$, X_H with $H \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ maximal, $X_{ns}^+(N)$ for $N = 2, 4, 8, 16$, and various other small genus modular curves.

We first assume that $-I \in H$. Let H_n be the nth subgroup in our list of 727 (as given in the file `gl2data.txt`), and let $X_n = X_{H_n}$. Instead of constructing the coverings $X_n \to X_1$ directly, we will instead construct coverings $X_n \to X_m$ so that H_n is a maximal subgroup of H_m and compose to get $X_n \to X_1$. In almost all cases the degree of the covering $X_n \to X_m$ is 2. (The exceptions are $X_6 \to X_1$, which has degree 3, and $X_7 \to X_1$, $X_{55} \to X_7$, and $X_{441} \to X_{55}$ which all have degree 4. The curves X_1, X_7, X_{55} and X_{441} are the curves $X_{ns}^+(2^k)$ for $1 \leq k \leq 4$).

In this process, if we find that X_n is a pointless conic, a pointless genus one curve, or an elliptic curve of rank zero, we do not compute any further coverings of X_n. For this reason, it is only necessary for us to compute models of X_n for 345 choices of n.

In Section 6.2 of [41], Shimura shows that the field L of modular functions on $X(N)$ whose Fourier coefficients at the cusp at infinity are contained in $\mathbb{Q}(\zeta_N)$ is generated by

$$f_{\vec{a}}(z) = \frac{9}{\pi^2} \frac{E_4(z)E_6(z)}{\Delta(z)} \wp_z\left(\frac{cz+d}{N}\right)$$

where $\vec{a} = (c, d)$ and $(c, d) \in (\mathbb{Z}/N\mathbb{Z})^2$ has order N. Here, $\wp_z(\tau)$ is the classical Weierstrass $\wp$-function attached to the lattice $\langle 1, z\rangle$.

Theorem 6.6 of [41] shows that the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ given by $f_{\vec{a}}|M = f_{\vec{a}M}$ uniquely extends to the entire field L and is an automorphism of L fixing $\mathbb{Q}(j)$. Moreover, $\mathrm{Gal}(K/\mathbb{Q}(j)) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$, and $\zeta_N|M = \zeta_N^{\det M}$. When $M \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, the action of M on K is $\mathbb{Q}(\zeta_N)$-linear and agrees with the usual action: if $h \in L$ and $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, then

$$(h|M)(z) = h\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right).$$

Given $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ containing $\Gamma(2^k)$, we can think of H as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ (by abuse of notation also called H) using the isomorphism $\mathbb{Z}_2/2^k\mathbb{Z}_2 \cong \mathbb{Z}/2^k\mathbb{Z}$. Let $\tilde{H}$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ containing H so that the covering $X_H \to X_{\tilde{H}}$ has minimal degree. Our goal is to find an element $h \in L$ that generates the fixed field of H over $\mathbb{Q}(X_{\tilde{H}})$, and compute its images under representatives for the right cosets of H in $\tilde{H}$.

We consider the $\mathbb{Q}(\zeta_{2^k})$-subspace V of L spanned by the functions $f_{\vec{a}}$. It is natural to seek a modular function h in the subspace of V fixed by H. However, this approach does not always succeed. The map $f_{\vec{a}} \to f_{\vec{a}} \cdot \frac{\Delta(z)}{E_4(z)E_6(z)}$ is a bijection between V and the space of weight 2 Eisenstein series for $\Gamma(2^k)$ with coefficients in $\mathbb{Q}(\zeta_{2^k})$ (see [19], Section 4.6) and the dimension of the space of weight 2 Eisenstein series for H is the number of cusps of X_H minus one (see equation (4.3) on page 111 of [19]). If there is a subgroup M with $H \subseteq M$ for which X_H and X_M have the same number of cusps, then $V^H = V^M$ and we will not succeed in finding a primitive element for $\mathbb{Q}(X_H)$. Instead, we will find a subgroup $K \subseteq H$ so that X_K has more cusps than X_M for any subgroup M with $K \subseteq M \subseteq H$ (with $K \neq M$). The number of cusps a subgroup K has is the number of orbits $K \cap \mathrm{SL}_2(\mathbb{Z}/2^k\mathbb{Z})$ has in its natural action on $\mathbb{P}^1(\mathbb{Z}/2^k\mathbb{Z})$. If $K \cap \mathrm{SL}_2(\mathbb{Z}/2^k\mathbb{Z}) = \Gamma(2^k)$, the action of K on $\mathbb{P}^1(\mathbb{Z}/2^k\mathbb{Z})$ will be trivial, and so K will have more cusps than any larger subgroup.

Once K is selected, we compute $V^{K\cap \mathrm{SL}_2(\mathbb{Z}/2^k\mathbb{Z})}$. The sum $\sum_{\vec{a}} f_{\vec{a}} \cdot \frac{\Delta(z)}{E_4(z)E_6(z)}$ over all vectors $\vec{a}$ with order 2^k in $(\mathbb{Z}/2^k\mathbb{Z})^2$ is fixed by $\mathrm{SL}_2(\mathbb{Z}/2^k\mathbb{Z})$ and is a holomorphic modular form of weight 2. Since there are no nonzero weight 2 modular forms for $\mathrm{SL}_2(\mathbb{Z})$, $\sum_{\vec{a}} f_{\vec{a}} = 0$. However, as proved by Hecke in [24], removing any one of these gives a linearly independent set. From this, we know exactly how $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ acts on the space V, and we can compute subspaces fixed by various subgroups in terms of a basis, and only compute Fourier expansions when needed. We use this to compute $V^{K\cap \mathrm{SL}_2(\mathbb{Z}/2^k\mathbb{Z})} = \langle w_1, w_2, \ldots, w_d\rangle$ by determining the $\mathbb{Q}(\zeta_{2^k})$-subspace of V fixed by generators of $K \cap \mathrm{SL}_2(\mathbb{Z}/2^k\mathbb{Z})$. Once this is computed, we determine $V^K = \langle x_1, x_2, \ldots, x_m\rangle$ (a $\mathbb{Q}$-subspace of V) by considering the action of generators of K on $\zeta^i w_j$. We select $x = \sum_{i=1}^m i x_i$ as a "random" element of V^K and verify that the number of images of x under the action of $\tilde{H}$ is equal to $[\tilde{H} : K]$.

Finally, we compute the Fourier expansions of the $f_{\vec{a}}$ and use these to compute the Fourier expansions of the images of x. If $g_1, g_2, \ldots, g_r$ are representatives for the right cosets of K in H, we define

$$h = e_s(x|g_1, x|g_2, \ldots, x|g_r),$$

where e_s is the degree s elementary symmetric polynomial in r variables. We start with $s = 1$ and check if there are $[\tilde{H} : H]$ images of h under the action of the right cosets of H in $\tilde{H}$. We increment s until this occurs (and find that in all cases we can take $s \leq 3$). We build the polynomial

$$F(t) = \prod_{g\in T}(t - h|g).$$

Each of the coefficients of $F(t)$ is an element of $\mathbb{Q}(X_{\tilde{H}})$, which can be recognized from their Fourier expansion. In the case that $X_{\tilde{H}}$ has genus one, we use the following result, whose proof is straightforward and we omit.

Lemma 4.2. *Let $E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve and $g\colon E \to \mathbb{P}^1$ be a degree k morphism. Then,*

$$g = \frac{P(x) + yQ(x)}{R(x)}$$

where P, Q and R are polynomials with $\deg P \leq 3k-3$, $\deg Q \leq 3k-5$ and $\deg R \leq 3k-3$.

We then have explicitly that $\mathbb{Q}(X_H) = \mathbb{Q}(X_{\tilde{H}})[t]/(F(t))$. At this point we use some straightforward techniques to simplify the model generated.

Example 4.3. We will consider the example of the covering $X_{57} \to X_{22}$. The subgroup H_{22} is an index 8, level 8 subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$. It is one of three maximal subgroups (up to $\mathrm{GL}_2(\mathbb{Z}_2)$ conjugacy) of H_7, which is the unique maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ of index 4. When the covering $X_{22} \to X_7$ was computed, we determined that $X_{22} \cong \mathbb{P}^1$ and we computed and stored the Fourier expansion of a function f_{22} with $\mathbb{Q}(X_{22}) = \mathbb{Q}(f_{22})$. The subgroup H_{57} is an index 2 subgroup of H_{22}, and $H_{57} \supseteq \Gamma(16)$. It is generated by $\Gamma(16)$ and the matrices

$$\begin{bmatrix} 11 & 4 \\ 8 & 3 \end{bmatrix}, \begin{bmatrix} 15 & 11 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 7 & 2 \\ 2 & 1 \end{bmatrix}, \text{ and } \begin{bmatrix} 15 & 15 \\ 1 & 0 \end{bmatrix}.$$

Both H_{22} and H_{57} have two cusps. We choose K to be the subgroup generated by $\Gamma(16)$ and the matrices

$$\begin{bmatrix} 13 & 2 \\ 14 & 11 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 15 & 0 \end{bmatrix}, \text{ and } \begin{bmatrix} 1 & 0 \\ 7 & 7 \end{bmatrix}.$$

We have $[H_{57} : K] = 4$. The modular curve X_K has 8 cusps. The subspace V of $\mathbb{Q}(X_{\Gamma(16)})$ is a $\mathbb{Q}(\zeta_{16})$-vector space of dimension 95 spanned by the $f_{\vec{a}}$, where $\vec{a} = (c, d) \in (\mathbb{Z}/16\mathbb{Z})^2$ and at least one of c or d is odd. The subspace fixed by $K \cap \mathrm{SL}_2(\mathbb{Z})$ has dimension 7. Let $g_1, g_2, \ldots, g_7$ be a basis for this space. We consider the 56-dimensional $\mathbb{Q}$-vector space spanned by $\{\zeta_{16}^i g_j : 0 \le i \le 7, 1 \le j \le 7\}$ and we find the 7-dimensional subspace fixed by the action of K. We select a linear combination of these 7 functions to obtain a "random" modular function $x(z)$ fixed by K.

This $x(z)$ is still represented as a linear combination of the functions $f_{\vec{a}}$. We now compute the q-expansions of $x(z)|\gamma$, where γ ranges over representatives of the 8 right cosets of K in H_{22}. We partition these into two sets,

$$\{x_1(z), x_2(z), x_3(z), x_4(z)\} \text{ and } \{x_1(z)|\delta, x_2(z)|\delta, x_3(z)|\delta, x_4(z)|\delta\}$$

where the $x_i(z)$ are the images of $x(z)$ under cosets of K contained in H_{57}, and $\delta \in H_{22}$ but $\delta \notin H_{57}$.

We plug the $x_i(z)$ into the second elementary symmetric polynomial to obtain a modular function $h(z)$ for H_{57}. Its image $h(z)|\delta$ under the action of δ is obtained from the $x_i(z)|\delta$. Finally, a generator for $\mathbb{Q}(X_{57})/\mathbb{Q}(X_{22})$ is obtained as a root of the polynomial

$$(x - h(z))(x - h(z)|\delta).$$

The function $f_{22}(z)$ with $\mathbb{Q}(X_{22}) = \mathbb{Q}(f_{22})$ has Fourier expansion

$$\begin{aligned} f_{22}(z) = {} & 3\sqrt{2} + (36 + 24\sqrt{2})(1 + i)q^{1/4} + (288 + 216\sqrt{2})iq^{1/2} \\ & -(480\sqrt{2} + 720)(1 - i)q^{3/4} - 96\sqrt{2}q + \cdots. \end{aligned}$$

The function $h(z) + h(z)|\delta$ has degree at most 3, and in fact we find that

$$h(z) + h(z)|\delta = \frac{2^{11} \cdot 3^3 \cdot \left(155f_{22}^2 - 5946f_{22} - 26784\right)}{f_{22}^2 + 12f_{22} + 30}.$$

Similarly, we find that

$$(h(z))(h(z)|\delta) = \frac{2^{20} \cdot 3^6 \cdot \left(174569f_{22}^4 - 739788f_{22}^3 + 26364168f_{22}^2 + 298652832f_{22} + 680985144\right)}{\left(f_{22}^2 + 12f_{22} + 30\right)^2}.$$

These equations show that there is a modular function g for X_{57} so that $g^2 = 18 - f_{22}^2$. This equation for X_{57} is a conic. Finding an isomorphism between this conic and $\mathbb{P}^1$ yields a function f_{57} for which $\mathbb{Q}(X_{57}) = \mathbb{Q}(f_{57})$. This f_{57} satisfies

$$f_{22} = \frac{3f_{57}^2 + 6f_{57} - 3}{f_{57}^2 + 1},$$

which gives the covering map $X_{57} \to X_{22}$. The entire calculation takes 26 seconds on a 64-bit 3.2 GHz Intel Xeon W3565 processor.

Taking, for example, $f_{57} = 0$ gives $f_{22} = -3$. Mapping from $X_{22} \to X_7 \to X_1$ gives $j = -320$. The smallest conductor elliptic curve with this j-invariant is

$$E\colon y^2 = x^3 - x^2 - 3x + 7,$$

and the 2-adic image for this curve is H_{57}.

5 The cases with $-I \notin H$

In this section we describe how to compute, for subgroups such that $-I \notin H$ and $g(X_H) = 0$, a family of curves E_t over an open subset $U \subset \mathbb{P}^1$ such that an elliptic curve E/K without CM has 2-adic image of Galois contained in a subgroup conjugate to H if and only if there exists $t \in U(K)$ such that $E_t \cong E$.

When $-I \in H$, the 2-adic image for E is contained in H if and only if the same is true of the quadratic twists E_D of E. For this reason, knowing equations for the covering map $X_H \to X_1$ is sufficient to check whether a given elliptic curve has 2-adic image contained in H.

When $-I \notin H$, more information is required. First, observe that if $-I \notin H$, then $\widetilde{H} = \langle -I, H\rangle$ is a subgroup with $[\widetilde{H} : H] = 2$ that contains H. Recall that the coarse spaces of X_H and $X_{\widetilde{H}}$ are isomorphic. In order for there to be non-trivial rational points on X_H, it must be the case that $X_{\widetilde{H}}(\mathbb{Q})$ contains non-cuspidal, non-CM rational points. A detailed inspection of the rational points in the cases that $-I \in H$ shows that this only occurs if $X_{\widetilde{H}}$ has genus zero. There are 1006 subgroups H that must be considered.

Since we are not interested in the cases of elliptic curves with CM, we will remove the points of X_H lying over $j = 0$ and $j = 1728$. Let $\pi : X_H \to \mathbb{P}^1$ be the map to the j-line and $U = \pi^{-1}(\mathbb{P}^1 - \{0, 12^3, \infty\}) \subset X_H$. Then points of U have no non-trivial automorphisms and as a consequence, U is fine moduli space (see Section 2). We let $E_H \to U$ denote the universal family of (non-CM) elliptic curves with 2-adic image contained in H. By Lemma 2.4 there is a model for E_H of the form

$$E_H\colon y^2 = x^3 + A(t)x + B(t)$$

where $A(t), B(t) \in \mathbb{Z}[t]$. Knowing that such a model exists, we will now describe how to find it.

Let K be any field of characteristic zero. Suppose that E/K is an elliptic curve corresponding to a rational point on X_H with $j(E) \notin \{0, 1728\}$ and given by

$$E\colon y^2 = x^3 + Ax + B.$$

Now, if

$$E_d\colon dy^2 = x^3 + Ax + B$$

is a quadratic twist of E, then E and E_d are isomorphic over $K(\sqrt{d})$ with the isomorphism sending $(x, y) \mapsto (x, y/\sqrt{d})$. Fix a basis for the 2-power torsion points on E and let $\rho_E\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}_2)$ be the corresponding Galois representation. Taking the image of the fixed basis on E under this isomorphism gives a basis on E_d, and with this choice of basis, we have

$$\rho_{E_d} = \rho_E \cdot \chi_d$$

where χ_d is the natural isomorphism $\mathrm{Gal}(K(\sqrt{d})/K) \to \{\pm I\}$. We can now state our next result.

Lemma 5.1. *Assume the notation above. Let $\widetilde{H}$ be the subgroup generated by the image of ρ and $-I$. Suppose $H \subset \widetilde{H}$ is a subgroup of index 2 with $-I \notin H$. Then there is a unique quadratic twist E_d so that the image of ρ_{E_d} (computed with respect to the fixed basis coming from E) lies in H.*

Remark 5.2. Without the chosen basis for the 2-power torsion on E_d, the statement is false. Indeed, it is possible for two different index two (and hence normal) subgroups N_1 and N_2 of $\widetilde{H}$ to be conjugate in $\mathrm{GL}_2(\mathbb{Z}_2)$. The choice of a different basis for the 2-power torsion on E_d would allow the image of ρ_{E_d} to be either N_1 or N_2.

Proof. Observe that $j(E) \notin \{0, 1728\}$ implies that $E \cong E_d$ if and only if $d \in (K^\times)^2$. Recall that $\rho_{E_d} = \rho_E \cdot \chi_d$.

Let L be the fixed field of $\{\sigma \in \mathrm{Gal}(\overline{K}/K) : \rho_E(\sigma) \in H\}$. Then since H is a subgroup of $\widetilde{H}$ of index at most 2, $[L : K] \leq 2$. If $\rho_E(\sigma) \notin H$, then $\rho_E(\sigma) \in (-I)H$. Thus, the image of ρ_{E_d} is contained in H if and only if $\chi_d(\sigma) = -1 \iff \sigma \notin \mathrm{Gal}(\overline{K}/L)$. Thus, the image of ρ_{E_d} is contained in H if and only if $L = K(\sqrt{d})$. This proves the claim. □

We start by constructing a model for an elliptic curve

$$E_t\colon y^2 = x^3 + A(t)x + B(t)$$

where $A(t), B(t) \in \mathbb{Z}[t]$ and $j(E_t) = p(t)$, where $p\colon X_{\widetilde{H}} \to X_1$ is the covering map from $X_{\widetilde{H}}$ to the j-line. By the above lemma, the desired model of E_H will be a quadratic twist of E_t, so

$$E_H\colon y^2 = x^3 + A(t)f(t)^2 + B(t)f(t)^3$$

for some squarefree polynomial $F(t) \in \mathbb{Z}[t]$. (Here, we say that a polynomial $F(t) \in \mathbb{Z}[t]$ is squarefree if whenever $F(t) = g(t)^2 h(t)$ with $g, h \in \mathbb{Z}[t]$, then $g = \pm 1$).

Given a set of primes S and an integer n, we define $\mathrm{sf}_S(n)$ to be the product of the primes that divide the squarefree part of n but which are not elements of S. (For example, when $S = \{2\}$, $\mathrm{sf}_S(24) = 3$).

Lemma 5.3. *Let $F(t) \in \mathbb{Z}[t]$ be squarefree and let $D(t) \in \mathbb{Z}[t]$. Suppose that for some finite set S of primes, $sf_S(F(n))$ divides $D(n)$ for all but finitely many $n \in \mathbb{Z}$. Then $F(t)$ divides $D(t)$ in $\mathbb{Q}[t]$.*

Proof. To begin, we note that $\mathrm{sf}_S(F(n))$ takes infinitely many distinct values. Indeed, infinitely many primes p split in the splitting field of F. Choose an integer n such that $p \mid F(n)$. If $p^2 \nmid F(n)$, then p divides the squarefree part of $F(n)$, proving the claim. Suppose that $p^2 \mid F(n)$. Since F is squarefree, for sufficiently large p, $p \nmid F'(n)$ (otherwise F would have a double root mod p). Since $F(n+p) \equiv F(n) + F'(n)p \pmod{p^2}$ we conclude that $p^2 \nmid F(n+p)$.

Next, we note that it suffices to assume that F is irreducible; indeed, if $F = F_1F_2$, then after enlarging S to include the primes dividing the resultant of F_1 and F_2, one has $\mathrm{sf}_S(F) = \mathrm{sf}_S(F_1)\mathrm{sf}_S(F_2)$, so the hypotheses of the lemma hold for each F_i.

We proceed by induction on $\deg D(t) + \deg F(t)$. If $D(t)$ is constant then the statement is trivial, since we can choose n such that the squarefree part of $F(n)$ has absolute value larger than $|D(n)|$, giving a contradiction unless $F(t)$ is also constant. If $\deg D(t) \geq \deg F(t)$, then by the division algorithm we can write

$$MD(t) = q(t)\,F(t) + r(t)$$

for some $M \in \mathbb{Z}$, $M \neq 0$ and $q(t), r(t) \in \mathbb{Z}[t]$ such that $\deg r(t) < \deg F(t)$. Enlarging S if necessary to include the primes that divide M, we see that $\mathrm{sf}_S(F(n)) | r(n)$ for all but finitely many n. By induction, this is a contradiction unless $r(t)$ is identically zero, in which case we have

$$MD(t) = q(t)\,F(t).$$

Finally, if $\deg D(t) < \deg F(t)$, then by the division algorithm we can write

$$MF(t) = q(t)\,D(t) + r(t)$$

for some $M \in \mathbb{Z}$ with $M \neq 0$ and $q(t), r(t) \in \mathbb{Z}[t]$ such that $\deg r(t) < \deg D(t)$. Again assuming that all prime divisors of M are in S, we see that $\mathrm{sf}_S(F(n)) | r(n)$ for all but finitely many integers n. By induction, this is a contradiction unless $r(t)$ is identically zero, in which case we have

$$MF(t) = q(t)\,D(t),$$

contradicting irreducibility of F. □

Theorem 5.4. *Let $F(t) \in \mathbb{Z}[t]$ be squarefree and such that E_H is isomorphic to the twist $E_{t,F(t)}$ of E_t by $F(t)$ and let $D(t)$ be the discriminant of the model E_t given above. Then $F(t) | D(t)$ in $\mathbb{Q}[t]$.*

Proof. We specialize, picking $n \in \mathbb{Z}$ so that E_n is non-singular. The 2-adic image for E_n is contained in $\widetilde{H}$. If K is the fixed field of H, then $K/\mathbb{Q}$ is a trivial or quadratic extension. If χ is the Kronecker character of K (resp. trivial character), then twisting E_n by χ will give a curve whose 2-adic image is contained in H.

Since $K \subseteq \mathbb{Q}(E_n[2^k])$ for some k, K must be unramified away from 2 and the primes dividing the conductor of E_n. Since the conductor of E_n divides the minimal discriminant

of E_n, and this in turn divides the discriminant of $E_n\colon y^2 = x^3 + A(n)x + B(n)$ (which is a multiple of 16), we have that if $K = \mathbb{Q}(\sqrt{d})$ with d squarefree, then $d|D(n)$. Moreover, d must be the squarefree part of $F(n)$. The theorem now follows from Lemma 5.3. □

Here is a summary of the algorithm we apply to compute the polynomial $F(t)$. Throughout, we will write $F(t) = cd(t)$, where $d(t)$ divides $D(t)$ in $\mathbb{Z}[t]$, $c \in \mathbb{Q}$ is squarefree, and $d(t)$ is not the zero polynomial mod any prime p.

(1) We pick an integral model for E_t and repeatedly choose integer values for t for which E_t is non-singular and does not have complex multiplication.
(2) For each such t, we compute a family of resolvent polynomials, one for each conjugacy class of $\tilde{H}$, that will allow us to determine the conjugacy class of $\rho_{E_t,2^k}(\mathrm{Frob}_p)$. (See Appendix A for a procedure to do this).
(3) We make a list of the quadratic characters corresponding to $\mathbb{Q}(\sqrt{d})$ for each squarefree divisor d of $2N(E_t)$. All twists of E_t with 2-adic image contained in H must be from this set.
(4) We compute the $\mathrm{GL}_2(\mathbb{Z}_2)$-conjugates of H inside $\widetilde{H}$. (For the $\widetilde{H}$ that we consider, computation reveals that there can be 1, 2, or 4 of these).
(5) We use the resolvent polynomials to compute the image of Frob_p for several primes p. Once enough primes have been used, it is possible to identify which twist of E_t has its 2-adic image contained in each $\mathrm{GL}_2(\mathbb{Z}_2)$-conjugate of H.
(6) The desired model of E_t will be a twist by $cd(t)$ for some divisor $d(t)$ of the discriminant. We keep a list of candidate values for c for each divisor $d(t)$ that work for all of the t-values tested so far, and eliminate choices of $d(t)$.
(7) We go back to the first step and repeat until the number of options remaining for pairs $(c, d(t))$ is equal to the number of $\mathrm{GL}_2(\mathbb{Z}_2)$-conjugates of H in $\widetilde{H}$. Each of these pairs $(c, d(t))$ gives a model for E_H. We output the simplest model found.

Remark 5.5. The algorithm above (step 5 in particular) sometimes requires a lot of decimal precision (in some cases as much as 8500 digits), and is in general fairly slow. Computing the equation for the universal curve over X_H is thus much slower than computing equations for X_H when $-I \in H$.

Example 5.6. There are two index 2 subgroups of H_{57} that do not contain $-I$. One of these, which we call H_{57a}, contains $\Gamma(32)$, and is generated by

$$\begin{bmatrix} 10 & 21 \\ 3 & 13 \end{bmatrix}, \begin{bmatrix} 15 & 1 \\ 27 & 2 \end{bmatrix}, \begin{bmatrix} 7 & 7 \\ 0 & 1 \end{bmatrix}.$$

We will compute E_H, the universal elliptic curve over H_{57a}. We let

$$E_t\colon y^2 = x^3 + A(t)x + B(t),$$

where

$$\begin{aligned} A(t) &= -6\left(725t^8 + 1544t^7 + 2324t^6 + 2792t^5 + 2286t^4 + 1336t^3 + 500t^2 + 88t + 5\right) \\ B(t) &= -32\left(3451t^{12} + 11022t^{11} + 22476t^{10} + 35462t^9 + 43239t^8 + 41484t^7 + 32256t^6\right. \\ &\quad \left. + 19596t^5 + 8601t^4 + 2630t^3 + 564t^2 + 78t + 5\right). \end{aligned}$$

These polynomials were chosen so that

$$j(E_t) = \frac{2^6\left(25t^4+36t^3+26t^2+12t+1\right)^3\left(29t^4+20t^3+34t^2+28t+5\right)}{\left(t^2-2t-1\right)^8} = p(t),$$

where $p\colon X_{57} \to X_1$ is the map to the j-line. There are four squarefree factors of the discriminant of E_t in $\mathbb{Q}[t]$:

$$1,\ t^2-2t-1,\ t^4+\frac{20}{29}t^3+\frac{34}{29}t^2+\frac{28}{29}t+\frac{5}{29},\ \text{and}\ \ t^6-\frac{38}{29}t^5-\frac{35}{29}t^4-\frac{60}{29}t^3-\frac{85}{29}t^2-\frac{38}{29}t-\frac{5}{29}.$$

We specialize E_t by taking $t = 1$, giving

$$E_t\colon y^2 = x^3 - 69600x + 7067648.$$

Considering H_{57} as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/32\mathbb{Z})$, it has 416 conjugacy classes. We compute the resolvent polynomials for each of these conjugacy classes and verify that they have no common factors. Since E_t has conductor $2^8 \cdot 3^2 \cdot 29^2$, the fixed field of H_{57a} inside $\mathbb{Q}(E_t[32])$ is a quadratic extension ramified only at 2, 3 and 29. There are sixteen such fields.

There are two index 2 subgroups of H_{57} that are $\mathrm{GL}_2(\mathbb{Z}_2)$-conjugate to H_{57a}. As a consequence, there are two quadratic twists of E_t whose 2-adic image will be contained in some conjugate of H_{57a}. By computing the conjugacy class of $\rho(\mathrm{Frob}_p)$ for $p = 53$, 157, 179 and 193, we are able to determine that those are the -87 twist and the 174 twist. This gives us a total of 8 possibilities for pairs $(c, d(t))$ (two for each $d(t)$).

Next, we test $t = 2$. This gives the curve

$$E_t\colon y^2 = x^3 - 4024542x + 3107583520.$$

This time, we find that the -4926 and 2463 twists are the ones whose 2-adic image is contained in H_{57a} (up to conjugacy). This rules out all the possibilities for the pairs $(c, d(t))$ except for two. These are $c = 174$ and $c = -87$ and $d(t) = t^6 - \frac{38}{29}t^5 - \frac{35}{29}t^4 - \frac{60}{29}t^3 - \frac{85}{29}t^2 - \frac{38}{29}t - \frac{5}{29}$. This gives the model

$$E_{H_{57a}}\colon y^2 = x^3 + \tilde{A}(t)x + \tilde{B}(t),$$

where

$$\tilde{A}(t) = 2\cdot 3^3\cdot\left(t^2-2t-1\right)^2\cdot\left(25t^4+36t^3+26t^2+12t+1\right)\left(29t^4+20t^3+34t^2+28t+5\right)^3$$

$$\tilde{B}(t) = 2^5\cdot 3^3\cdot\left(t^2-2t-1\right)^3\cdot\left(t^2+1\right)\cdot\left(7t^2+6t+1\right)\cdot\left(17t^4+28t^3+18t^2+4t+1\right)$$
$$\cdot\quad\left(29t^4+20t^3+34t^2+28t+5\right)^4.$$

In total, this calculation takes 3 hours and 46 minutes.

The smallest conductor that occurs in this family is 6400. The curve $E\colon y^2 = x^3 + x^2 - 83x + 713$ and its -2-quadratic twist $E'\colon y^2 = x^3 + x^2 - 333x - 6037$ both have conductor 6400 and 2-adic image H_{57a}.

6 A curious example

Before our exhaustive analysis of the rational points on the various X_H, we pause to discuss the following curious example, which demonstrates that Hilbert's irreducibility theorem does not necessarily hold when the base is an elliptic curve with positive rank.

One expects that if $X_H(\mathbb{Q})$ is infinite then there exist infinitely many elliptic curves $E/\mathbb{Q}$ such that $\rho_E(G_{\mathbb{Q}})$ is actually *equal* to H. The following example shows that this is not necessarily true.

Example 6.1. The subgroup H_{155} is an index 24 subgroup containing $\Gamma(16)$ generated by

$$\begin{bmatrix} 1 & 3 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 12 & 3 \end{bmatrix}, \text{ and } \begin{bmatrix} 1 & 1 \\ 12 & 7 \end{bmatrix}.$$

The curve X_{155} is an elliptic curve

$$X_{155}\colon y^2 = x^3 - 2x$$

and $X_{155}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ and is generated by $(0,0)$ and $(-1,-1)$. The map from X_{155} to the j-line is given by $j(x,y) = \frac{256(x^4-1)^3}{x^4}$.

Since the two-torsion subgroup $X_{155}(\mathbb{Q})[2]$ is non-trivial (as imposed by Remark 7.2), X_{155} has an étale double cover $\phi\colon E \to X_{155}$ defined over $\mathbb{Q}$ and such that E has good reduction away from 2. By the Riemann-Hurwitz formula, E has genus 1; the map is thus a 2-isogeny and $E(\mathbb{Q})$ thus has rank one. By étale descent (see Subsection 7.3), since X_{155} and E have good reduction outside of 2, every point of $X_{155}(\mathbb{Q})$ lifts to $E_d(\mathbb{Q})$ for $d \in \{\pm 1, \pm 2\}$. It turns out that for each such d, there is an index 2 subgroup $H_d \subset H_{155}$ such that $E_d \cong X_{H_d}$. (These are X_{284}, X_{318}, X_{328} and X_{350}, respectively). It follows that

$$\bigcup_{d \in \{\pm 1, \pm 2\}} \phi_d(E_d(\mathbb{Q})) = X_{H_{155}}(\mathbb{Q}).$$

In particular, for every point in $X_{H_{155}}(\mathbb{Q})$, the 2-adic image of Galois of the corresponding elliptic curve is contained in one of the four index two subgroups H_d!

Remark 6.2. We note that if $X_H \cong \mathbb{P}^1$, then since $\mathbb{P}^1$ has no étale covers and since there is a finite collection of subgroups $H_1, \dots, H_n$ such that any K properly contained in H is a subgroup of some H_i, the image

$$\bigcup_{K \subset H} \phi_K(X_K(\mathbb{Q})) = \bigcup_{i=1}^{n} \phi_{H_i}(X_{H_i}(\mathbb{Q})) \subset X_H(\mathbb{Q})$$

(where ϕ_K is the map $X_K \to X_H$ induced by the inclusion $K \subset H$) is a thin set, and in particular most (i.e. a density one set) of the points of $X_H(\mathbb{Q})$ correspond to $E/\mathbb{Q}$ such that $\rho_E(G_{\mathbb{Q}}) = H$.

Remark 6.3. There are seven genus one curves X_H that are elliptic curves of positive rank where the corresponding subgroup H has index 24. In all seven cases, all of the rational points lift to modular double covers (although it is not always the case that all four twists have local points). In fact, every one of the 20 modular curves X_H, where H has index 48 and for which $X_H(\mathbb{Q})$ is a positive rank elliptic curve is a double cover of one of these seven curves.

This example is more than just a curiosity; it inspired the technique of Subsection 7.4 which allows us to determine the rational points on most of the genus 5 and 7 curves.

This example also raises the following question.

Question 6.4. Do there exist infinite unramified towers of modular curves such that each twist necessary for étale descent is modular?

If so, this would imply that none of the curves in such a tower have non-cuspidal non-CM points. A potential example is the following: the Cummins/Pauli database [15] reveals that there might be such a tower starting with $16A^2, 16B^3, 16B^5, 16B^9, 16A^{17}$. There is then a level 32, index 2 subgroup of $16A^{17}$ that has genus 33.

7 Analysis of rational points - theory

The curves whose models we computed above have genera either 0,1,2,3,5,7; see Table 2.

For the genus 0 curves, we determine whether the curve has a rational point, and if so we compute an explicit isomorphism with $\mathbb{P}^1$. For the genus 1 curves, we determine whether the curve has a rational point, and if so compute a model for the resulting elliptic curve and determine its rank and torsion subgroup. This is straightforward: all covering maps except 4 have degree 2, so we end up with a model of the form $y^2 = p(t)$, where $p(t)$ is a polynomial, and the desired technique is implemented in Magma. The remaining 4 cases are handled via a brute force search for points.

In the higher genus cases, we determine the complete set of rational points. Each of the following techniques play a role:

(1) local methods,
(2) Chabauty for genus 2 curves,
(3) elliptic curve Chabauty,
(4) étale descent,
(5) "modular" étale double covers of genus 5 and 7 curves, and
(6) an improved algorithm for computing automorphisms of curves.

In this section we describe in detail the theory behind the techniques used to analyze the rational points on the higher genus curves. The remainder of the paper is a case by case analysis of the rational points on the various X_H.

Remark 7.1. Facts about rational points on X_H

(1) Every rational point on a curve X_H of genus one that has rank zero is a cusp or a CM point.

Table 2 Summary of the computation of the 727 models

Type	Number
$X_H \cong \mathbb{P}^1$	175
Pointless conics	10
Elliptic curves with positive rank	27
Elliptic curves with rank zero	25
Genus 1 curves computed with no points	6
Genus 1 curves whose models are not necessary	165
Genus 2 models computed	57
Genus 2 curves whose models are not necessary	40
Genus 3 models computed	22
Genus 3 curves whose models are not necessary	142
Genus 5 models computed	20
Genus 5 curves whose models are not necessary	24
Genus 7 models computed	4
Genus 7 curves whose models are not necessary	10

(2) The only genus 2 curve with non-cuspidal, non-CM rational points is X_{441}, also known as $X_{ns}^{+}(16)$. This curve has two non-cuspidal, non-CM rational points, with distinct j-invariants.
(3) The only genus 3 curves with non-cuspidal, non-CM rational points are X_{556}, X_{558}, X_{563}, X_{566}, X_{619}, X_{649}. Each of these gives rise to a single, distinct j-invariant.
(4) All the rational points on the genus 5 and 7 curves are either cusps or CM points.

Remark 7.2. The following observation powers many of these approaches – since Jacobians of 2-power level modular curves have good reduction outside of 2, each Jacobian is "forced" to have a non-trivial two torsion point (and more generally forced to have small mod 2 image of Galois). Indeed, the two division field $\mathbb{Q}(J[2])$ is unramified outside of 2, and there are few such extensions of small degree. In [26], it is shown that if $[K:\mathbb{Q}] \leq 16$ and $K/\mathbb{Q}$ is ramified only at 2, then $[K:\mathbb{Q}]$ is a power of 2. In particular, there are no degree 3 or 6 extensions of $\mathbb{Q}$ ramified only at 2, so an elliptic curve with conductor a power of 2 has a rational 2-torsion point. (In practice of course one can often compute directly the torsion subgroup of the Jacobian, by computing the torsion mod several primes, and then explicitly finding generators.) We remark that there is, however, a degree 17 extension of $\mathbb{Q}$ ramified only at 2, arising from the fact that the class number of $\mathbb{Q}(\zeta_{64})$ is 17.

7.1 Chabauty

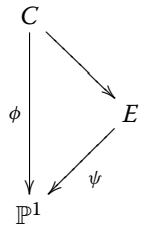
See [34] for a survey. The practical output is that

if $\operatorname{rk} \mathrm{Jac}_X(\mathbb{Q}) < \dim \mathrm{Jac}_X = g(X)$, then p-adic integration produces explicit 1-variable power series $f \in \mathbb{Q}_p[\![t]\!]$ whose set of $\mathbb{Z}_p$-solutions contains all of the rational points. This is all implemented in Magma for genus 2 curves over number fields, which will turn out to be the only case needed. See the section below on genus 2 curves for a complete discussion.

7.2 Elliptic chabauty

Given an elliptic curve E over a number field K of degree $d > 1$ over $\mathbb{Q}$ and a map $E \xrightarrow{\pi} \mathbb{P}^1_K$, one would like to determine the subset of $E(K)$ mapping to $\mathbb{P}^1(\mathbb{Q})$ under π. A method analogous to Chabauty's method provides a partial solution to this problem under the additional hypothesis that $\operatorname{rank} E(K) < d$ (and has been completely implemented in Magma). The idea is to expand the map $E \to \mathbb{P}^1_K$ in p-adic power series and analyze the resulting system of equations using Newton polygons or similar tools. See [8, 9] for a succinct description of the method and instructions for use of its Magma implementation.

A typical setup for applications is the following.



We have a higher genus curve C whose rational points we want to determine, and we have a particular map $C \to \mathbb{P}^1$ which is defined over $\mathbb{Q}$ and which factors through an elliptic

curve E over a number field K (but does not necessarily factor over $\mathbb{Q}$). Then any K-point of E which is the image of a $\mathbb{Q}$-point of C has rational image under $E \to \mathbb{P}^1$, exactly the setup of elliptic curve Chabauty. (Finding the factorization $C \to E$ can be quite tricky; see Subsection 9.3 for an example).

7.3 Étale descent

Étale descent is a "going up" style technique, first studied in [12] and [52] and developed as a full theory (especially the non-abelian case) in [44]. It is now a standard technique for resolving the rational points on curves (see e.g. [8, 21]) and lies at the heart of the modular approach to Fermat's last theorem (see [36], 5.6).

Let $\pi : X \to Y$ be an étale cover defined over a number field K such that Y is the quotient of some free action of a group G on X. Then there exists a finite collection $\pi_1 : X_1 \to Y, \ldots, \pi_n : X_n \to Y$ of twists of $X \to Y$ such that

$$\bigcup_{i=1}^{n} \pi_i(X_i(K)) = Y(K).$$

Moreover, if we let S be the union of the set of primes of bad reduction of X and Y and of the primes of $\mathcal{O}_K$ over the primes dividing $\#G$, then the cocycles corresponding to the twists are unramified outside of S. (See e.g. [44], 5.3).

We will use this procedure only in the case of étale double covers. In this case, $G = \mathbb{Z}/2\mathbb{Z}$ and, since the twists are consequently quadratic, we will instead denote twists of a double cover $X \to Y$ by $X_d \to Y$, where $d \in K^\times / \left(K^\times\right)^2$, and the above discussion gives that, for any point P of $Y(K)$, there will exist $d \in \mathcal{O}_{K,S}^\times / (\mathcal{O}_{K,S}^\times)^2$ such that P lifts to a point of $X_d(K)$.

7.4 Étale descent via double covers with modular twists

The following variant of Example 6.1 will allow us to resolve the rational points on some of the high genus curves.

We will occasionally be in the following setup: $K \subset H \subset \mathrm{GL}_2(\mathbb{Z}_2)$ are a pair of open subgroups such that $g(X_H) > 1$ and the corresponding map $X_K \to X_H$ is an étale double cover. By étale descent (see Subsection 7.3), since X_H and X_K have good reduction outside of 2, every point of $X_H(\mathbb{Q})$ lifts to a rational point on a quadratic twist $X_{K,d}(\mathbb{Q})$ for $d \in \{\pm 1, \pm 2\}$, so that

$$\bigcup_{d \in \{\pm 1, \pm 2\}} \phi_d(X_{K,d}(\mathbb{Q})) = X_H(\mathbb{Q}),$$

where $X_K \to X_H$ is induced by the inclusion $K \subset H$ and ϕ_d is the twist of this by d.

It turns out that, additionally, for each such d there is an index 2 subgroup $K_d \subset H$ such that $X_{K_d} \cong X_{K,d}$; i.e. each of the quadratic twists are also modular. Finally, a third accident occurs: each of the subgroups K_d is contained in a subgroup L_d such that X_{L_d} either has genus 1 and has no rational point, is an elliptic curve of rank zero, or is a genus zero curve with no rational points. In particular, since the inclusion of subgroups $K_d \subset L_d$ induces a map $X_{K_d} \to X_{L_d}$, this determines all of the rational points on each twist X_{K_d}, and thus on X_H.

This phenomenon occurs for 16 of the 20 subgroups H for which X_H has genus 5, and all four of the cases when X_H has genus 7. See Subsection 10.3 for details.

7.5 Constructing automorphisms of curves over number fields

If C is a curve of genus g and $D \to C$ is a degree n étale cover of C, then the genus of D is $ng - (n-1)$. In order to analyze rational points on D, it is very helpful to be able to find maps from D to curves of lower genus. In this context, it is helpful to compute the group G of automorphisms of D and consider quotients D/H for subgroups $H \subseteq G$.

Magma's algebraic function field machinery is able to compute automorphism groups of curves. However, the performance of these routines varies quite significantly based on the complexity of the base field. The routines work quickly over finite fields, but are often quite slow over number fields, especially when working with curves that have complicated models.

For our purposes, we are interested in quickly constructing automorphisms (defined over $\overline{\mathbb{Q}}$) of non-hyperelliptic curves $D/\mathbb{Q}$ with genus ≥ 3. (Magma has efficient, specialized routines for genus 2 and genus 3 hyperelliptic curves.) Our goal is not to provably compute the automorphism group, but to efficiently construct all the automorphisms that likely exist. The procedure we use is the following.

(1) Given a curve $D/\mathbb{Q}$, use Magma's routines to compute $\mathrm{Aut}(D/\mathbb{F}_p)$ for several different choices of primes p. If all automorphisms of D are defined over the number field K, then we expect that if p splits completely in K, then $|\mathrm{Aut}(D/\mathbb{F}_p)| = |\mathrm{Aut}_{\overline{\mathbb{Q}}}(D)|$. Data for several primes will give a prediction for $|\mathrm{Aut}_{\overline{\mathbb{Q}}}(D)|$ and K.

(2) Consider the canonical embedding of $D \subset \mathbb{P}^{g-1}$. Any automorphism of D can be realized as a linear automorphism of $\mathbb{P}^{g-1}$ that fixes the canonical image of D.

(3) Construct the "automorphism scheme" $X/\mathbb{Q}$ of linear automorphisms from $\mathbb{P}^{g-1}$ that map D to itself. Let $I(D) \subseteq \mathbb{Q}[x_1, x_2, \ldots, x_g]$ denote the ideal of polynomials that vanish on the canonical image of D. For each homogeneous generator f_i of $I(D)$ of degree d_i, we construct a basis $v_1^{(i)}, v_2^{(i)}, \ldots, v_{e_i}^{(i)}$ for the degree d_i graded piece of $I(D)$. If $\phi\colon D \to D$ is an automorphism, then

$$\phi(f_i) = \sum_{j=1}^{e_i} c_{i,j} v_j^{(i)}.$$

We construct the automorphism scheme as a subscheme of $\mathbb{A}^d$, where $d = g^2 + \sum_i d_i + 1$. We use g^2 variables for the linear transformation, $\sum_i d_i$ variables for the constants $c_{i,j}$ in the above equation, and one further variable to encode the multiplicative inverse of the determinant of the linear transformation. (This scheme actually has dimension 1 since an arbitrary scaling of the matrix is allowed.) We will extend X to a scheme over $\mathrm{Spec}\mathbb{Z}$ (which we also call X).

(4) Choose a prime p that splits completely in K and a prime ideal $\mathfrak{p}$ of norm p in $\mathcal{O}_K$, the ring of integers in K. Use Magma's routines to compute $\mathrm{Aut}(D/\mathbb{F}_p)$ and represent these automorphisms as points in $X(\mathbb{F}_p)$.

(5) Use Hensel's lemma to lift the points on $X(\mathbb{F}_p)$ to points on $X(\mathbb{Z}/p^r\mathbb{Z})$ for some modestly sized integer r. (We frequently use $r = 60$). Hensel's lemma is already implemented in Magma via `LiftPoint`.

(6) Scale the lifted points so that one nonzero coordinate is equal to 1. Then use lattice reduction to find points in K of small height that reduce to the points in $X(\mathbb{Z}/p^r\mathbb{Z})$

modulo $\mathfrak{p}^r$. Use these to construct points in $X(K)$, i.e., automorphisms of D defined over K.

The above algorithm runs very quickly in practice for curves of reasonably small genus. For example, the genus 5 curve given by

$$\begin{aligned} -2705a^2 + 1681b^2 - 1967bc + 2048c^2 - 2d^2 &= 0 \\ 73a^2 - 41b^2 + 64bc - 64c^2 - 2de &= 0 \\ -2a^2 + b^2 - 2bc + 2c^2 - 2e^2 &= 0 \end{aligned}$$

is one of the étale double covers of X_{619}. This curve has (at least) 16 automorphisms defined over $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ which are found by the above algorithm in 25.6 seconds. However, Magma's built in routines require a long time to determine the automorphism group (the routine did not finish after running it for 3 and 1/2 days).

7.6 Fast computation of checking isomorphism of curves

A related problem to computing automorphisms is proving that two curves are isomorphic. There are many instances of non-conjugate subgroups H and K with $X_H \cong X_K$. Within the 22 genus three curves, there are at most 7 isomorphism classes. Within the 20 genus five curves, there are at most 10 isomorphism classes. The 4 genus seven curves fall into two isomorphism classes.

Magma's built-in command `IsIsomorphic` suffices for hyperelliptic curves and a few higher genus curves that happen to have nice models. The simplest way to determine if two non-hyperelliptic genus 3 curves are isomorphic is to compute their canonical models and apply `MinimizeReducePlaneQuartic` and inspect the resulting simplified polynomials - at this point the isomorphisms can be seen by inspection.

In the genus 5 case, we use a variant of the approach described for automorphisms, and, given two curves C_1 and C_2, we construct an "isomorphism scheme" in a similar way to the automorphism scheme above. Again, we use Magma's internal commands to find isomorphisms mod p, and lift these to characteristic zero isomorphisms. In the genus 7 case, Magma's built-in commands are the most efficient.

7.7 Probable computation of ranks

It is straightforward to compute the rank of a curve of genus at most 2 using Magma's preexisting commands (e.g. via `RankBound`, an implementation of [46]); computation of the rank of the Jacobian of a genus 3 plane curve has recently been worked out [7], but is often impractical [7, Remark 1.1] and moreover has not been implemented in a publicly available way. For genus > 3 little is known in general (though special cases such as cyclic covers of $\mathbb{P}^1$ are known [37, 50]).

For the determination of the rational points on each X_H, we will only need a rigorous computation of rank for genus at most 2. Nonetheless, in many cases we can compute "probable" ranks, and mention this in the discussion as an indication of why we chose a particular direction of analysis. If H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ that contains $\Gamma(2^k)$, then X_H is a quotient of $X_1(4^k)$, but the map from $X_1(4^k) \to X_H$ is only defined over $\mathbb{Q}(\zeta_{4^k})$. For this reason, we cannot immediately conclude that each factor A of $\mathrm{Jac}\, X_H$ is modular. However, numerical data suggests that each such A is indeed a factor of $\mathrm{Jac}\, X_1(4^k)$. We can find a candidate for the corresponding modular form f (e.g. by comparing traces)

and compute a guess for the analytic rank, but we cannot prove that $A \cong A_f$, or that the algebraic and analytic ranks of A_f agree.

8 Analysis of rational points - genus 2

In the remaining sections we provably compute all of the rational points on each modular curve. Magma code verifying the below claims is available at [38] and additionally at the arXiv page of this paper.

There are 57 arithmetically maximal genus 2 curves. Among these, 46 have Jacobians with rank 0, 3 with rank 1, and 8 with rank 2. We will use étale descent on the rank 2 cases and Chabauty on the others. In each case, the rank of the Jacobian is computed with Magma's `RankBound` command. See the transcript of computations for full details, and see [11] for a detailed discussion of all practical techniques for determining the rational points on a genus 2 curve.

8.1 Rank 0

If $\mathrm{rk}\,\mathrm{Jac}_X(\mathbb{Q}) = 0$ then $\mathrm{Jac}_X(\mathbb{Q})$ is torsion. To find all of the rational points on X it thus suffices to compute the torsion subgroup of $\mathrm{Jac}_X(\mathbb{Q})$ and compute preimages of these under an inclusion $X \hookrightarrow \mathrm{Jac}_X$. This is implemented in Magma as the `Chabauty0(J)` command, and in each case Magma computes that the only rational points are the known points.

8.2 Rank 1

If $\mathrm{rk}\,\mathrm{Jac}_X(\mathbb{Q}) = 1$ then one can attempt Chabauty's method. This is implemented in Magma as the `Chabauty(ptJ)` command, and in each case Magma computes that the only rational points are the known points.

8.3 Rank 2

If $\mathrm{rk}\,\mathrm{Jac}_X(\mathbb{Q}) = 2$ then Chabauty's method doesn't apply and the analysis is more involved; instead we proceed by étale descent. In each case, the Jacobian of X has a rational 2-torsion point. Thus, given a model

$$X\colon y^2 = f(x)$$

of X, f factors as $f_1 f_2$, where both are polynomials of positive degree (and both of even degree if f has even degree), and X admits étale double covers $C_d \to X$, where the curve C_d is given by

$$\begin{aligned} C_d\colon\ dy_1^2 &= f_1(x) \\ dy_2^2 &= f_2(x) \end{aligned}$$

Since X has good reduction outside of 2 and the 2-cover $C_1 \to X$ is étale away from 2 (since it is the pullback of a 2-isogeny $A \to \mathrm{Jac}_X$, and such an isogeny is étale away from 2), by étale descent (see 7.3 above) every rational point on X lifts to a rational point on $C_d(\mathbb{Q})$ for $d \in \{\pm 1, \pm 2\}$. The Jacobian of C_d is isogenous to $\mathrm{Jac}_X \times E_d$, where E_d is the Jacobian of the (possibly pointless) genus one curve $dy_2^2 = f_2(x)$ (where we assume that $\deg f_2 \geq \deg f_1$, so that $\deg f_2 \geq 3$).

There are 4 isomorphism classes of genus 2 curves in our list with Jacobian of rank 2 ($X_{395}, X_{402}, X_{441}, X_{520}$). In two cases ($X_{395}$ and X_{402}), each twist C_d maps to a rank 0

elliptic curve. For example, X_{395} is the hyperelliptic curve $y^2 = x^6 - 5x^4 - 5x^2 + 1 = (x^2 - 2x - 1)(x^2 + 1)(x^2 + 2x - 1)$. This admits étale covers by the genus 3 curves

$$\begin{aligned} C_d\colon dy_1^2 &= x^2 + 1 \\ dy_2^2 &= (x^2 - 2x - 1)(x^2 + 2x - 1) \end{aligned}$$

each of which in turn maps to the genus 1 curve $E_d : dy_2^2 = (x^2 - 2x - 1)(x^2 + 2x - 1)$, and for $d \in \{\pm 1, \pm 2\}$, $\mathrm{rk}\,\mathrm{Jac}_{E_d} = 0$, allowing the determination the rational points on each C_d and thus on X_{395}.

For the remaining genus 2 curves, three of the twists map to a rank 0 elliptic curve, but the twist by -2 maps to a rank 1 elliptic curve. Here one may apply étale descent again, but over a quadratic extension. For example, X_{441} is the hyperelliptic curve $y^2 = x^6 - 3x^4 + x^2 + 1 = (x - 1)(x + 1)(x^4 - 2x^2 - 1)$. (This is the curve $X_{\mathrm{ns}}^+(16)$ whose non-cuspidal points classify elliptic curves whose mod 16 image of Galois is contained in the normalizer of a non-split Cartan subgroup. The rational points on this curve are resolved in [3] via elliptic Chabauty; we give an independent determination of the rational points on this curve.) This admits étale covers by the genus 3 curves

$$\begin{aligned} C_d\colon dy_1^2 &= (x - 1)(x + 1) \\ dy_2^2 &= (x^4 - 2x^2 - 1) \end{aligned}$$

The Jacobian of $dy_2^2 = x^4 - 2x^2 - 1$ has rank 0 for $d = \pm 1, 2$. For $d = -2$, we note that since $x^4 - 2x^2 - 1$ factors over $\mathbb{Q}(\sqrt{2})$ as $((x - 1)^2 - \sqrt{2})((x - 1)^2 + \sqrt{2})$, C_{-2} admits a further étale double cover over $\mathbb{Q}(\sqrt{2})$ by

$$\begin{aligned} X_{-2,d'}\colon \quad -2y_1^2 &= (x - 1)(x + 1) \\ -2d'y_2^2 &= (x - 1)^2 - \sqrt{2} \\ d'y_3^2 &= (x - 1)^2 + \sqrt{2} \end{aligned}$$

(Note that a priori one expects this factorization to occur over a small field by Remark 7.2). By descent theory, every rational point on C_{-2} lifts to a $K := \mathbb{Q}(\sqrt{2})$ point on $X_{-2,d'}$ for some $d' \in \mathcal{O}_{K,S}^\times / \left(\mathcal{O}_{K,S}^\times\right)^2$. These each map to the two genus 1 curves $d'y^2 = (x - 1)(x + 1)((x - 1)^2 - \sqrt{2})$ and $-2d'y^2 = (x - 1)(x + 1)((x - 1)^2 + \sqrt{2})$. For 6 of the 8 such d', one of these curves has rank 0, and for 2 both have rank 1. Any point coming from a rational point on X_{441} has rational x-coordinate, and elliptic Chabauty (as described in Subsection 7.2) successfully resolves the rational points on the remaining two curves.

9 Analysis of rational points - genus 3

There are 18 genus 3 curves (and at most 7 isomorphism classes).

Of the isomorphism classes, X_{556}, X_{558} are hyperelliptic and handled by étale descent; X_{618} admits a map to a rank zero elliptic curve defined over $\mathbb{Q}(\sqrt{2})$; X_{628}, X_{641}, and X_{650} have nice models and can be handled in a direct, ad hoc manner. Finally, X_{619} is the most difficult case – it has six rational points and its Jacobian has (probable) analytic rank 3; we are nonetheless able to handle this curve via an elliptic Chabauty argument whose setup is non-trivial. All other genus 3 curves on our list are isomorphic to one of these.

Remark 9.1. Unfortunately, consideration of Prym varieties (see [10] for a discussion) do not simplify analysis of any of the above curves; for instance, X_{619} admits an étale double cover, but one of the twists of the associated Prym varieties has rank 2.

9.1 Genus 3 hyperelliptic

The genus 3 curves $X_{556}, X_{558}, X_{563}, X_{566}$ are hyperelliptic. The last two curves are isomorphic to the first two, which are given by

$$X_{556}\colon y^2 = x^7 + 4x^6 - 7x^5 - 8x^4 + 7x^3 + 4x^2 - x$$
$$X_{558}\colon y^2 = x^8 - 4x^7 - 12x^6 + 28x^5 + 38x^4 - 28x^3 - 12x^2 + 4x + 1$$

Their Jacobians have rank 1, but unfortunately much of the machinery necessary to do Chabauty on curves of genus $g > 2$ is not implemented in Magma (e.g., a simple search did not reveal generators for the Jacobian of X_{556}; for a genus 2 curve one can efficiently search on the associated Kummer surface, but the analogous computation for abelian threefolds is not implemented).

Instead, we proceed by descent. The hyperelliptic polynomials both factor, so each X admits an étale double cover which itself admits a map to a genus 2 curve. Rational points on the genus 3 curves lift to twists of the étale double cover by $d \in \{\pm 1, \pm 2\}$. For example, X_{556} admits étale double covers by the genus 5 curves

$$\begin{aligned} C_d\colon dy_1^2 &= x \\ dy_2^2 &= (x-1)(x+1)(x^4 + 4x^3 - 6x^2 - 4x + 1) \end{aligned}$$

which each maps to the genus 2 hyperelliptic curve

$$H_d\colon dy^2 = (x-1)(x+1)(x^4 + 4x^3 - 6x^2 - 4x + 1).$$

For $d \in \{\pm 1, \pm 2\}$ the Jacobian of H_d has rank 0 or 1, and Chabauty reveals that any rational point on X_{556} is either a point at infinity or satisfies $x = 0$ or $y = 0$. Similarly, the defining polynomial of X_{558} factors as $(x^2 - 2x - 1)(x^2 + 2x - 1)(x^4 - 4x^3 - 6x^2 + 4x + 1)$, and each of the four resulting genus 2 hyperelliptic curves

$$dy^2 = \left(x^2 + 2x - 1\right)\left(x^4 - 4x^3 - 6x^2 + 4x + 1\right)$$

have Jacobians of rank 1.

Each of these four hyperelliptic curves has four non-cuspidal, non-CM rational points that all have the same image on the j-line. For X_{556} we obtain $j = 2^4 \cdot 17^3$, for X_{558} we obtain $j = \frac{4097^3}{16}$, for X_{563} we obtain $j = 2^{11}$, and for X_{566} we obtain $j = \frac{257^3}{256}$.

9.2 Analysis of X_{618}

The curve X_{618} has two visible rational points.

Over the field $\mathbb{Q}(\sqrt{2})$, X_{618} maps to the elliptic curve

$$E\colon y^2 = x^3 + \left(\sqrt{2} + 1\right)x^2 + \left(-3\sqrt{2} - 5\right)x + \left(-2\sqrt{2} - 3\right)$$

which has rank 0 over $\mathbb{Q}(\sqrt{2})$ and has four $\mathbb{Q}(\sqrt{2})$-rational points, two of which lift to rational points of X_{618}.

We found this cover by computing $\mathrm{Aut}\, X_{618,\mathbb{Q}(\sqrt{2})}$ (which has order 8) and computing E as the quotient of $X_{618,\mathbb{Q}(\sqrt{2})}$ by one of these automorphisms. (See Subsection 7.5 for a description of this computation).

9.3 Analysis of X_{619}

The above techniques do not work on X_{619}; its Jacobian has (probable) analytic rank 3 and, while it admits an étale double cover D, a twist of D has rational points and associated Prym variety of rank 2. The curve D_δ has the equation

$$\begin{aligned}\delta r^2 &= -2705u^2 + 1681v^2 - 1967vw + 2048w^2\\ \delta rs &= 73u^2 - 41v^2 + 64vw - 64w^2\\ \delta s^2 &= -2u^2 + v^2 - 2vw + 2w^2.\end{aligned}$$

A bit of work reduces this to an elliptic Chabauty computation. Over the quartic field $K = \mathbb{Q}(a)$, where $a = \sqrt{(2+\sqrt{(2)})}$, any quadratic twist D_δ of D has automorphism group $D_8 \times \mathbb{Z}/2\mathbb{Z}$. Let H be the subgroup $\langle \iota_1, \iota_2\rangle$, where $\iota_1 : D_\delta \to D_\delta$ is given by $\iota_1(u:v:w:r:s) = (u:-v:-w:r:s)$ and

$$\begin{aligned}\iota_2(u:v:w:r:s) = \Bigg(u : \frac{\sqrt{2}}{2}v - w : -\frac{1}{2}v - \frac{\sqrt{2}}{2}w :\\ \frac{1}{18}\left(-73a^3+228a\right)r + \frac{1}{18}\left(-2624a^3+8529a\right)s : \frac{1}{9}\left(a^3-3a\right)r + \frac{1}{18}\left(73a^3-228a\right)s\Bigg).\end{aligned}$$

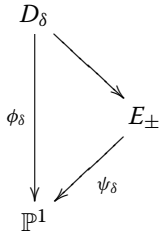
The twist D_{-2} has no $\mathbb{Q}_2$ points. When $\delta = 1$ or 2, the quotient D_δ/H is isomorphic to the elliptic curve

$$\begin{aligned}E_+ : \delta y^2 = {} & x^3 + \left(a^3+1\right)x^2 + \left(194a^3 + 153a^2 - 660a - 509\right)\\ & \times x + \left(-1815a^3 - 1389a^2 + 6202a + 4747\right)\end{aligned}$$

and the quotient D_{-1}/H is isomorphic to the elliptic curve

$$E_- : \delta y^2 = x^3 + \left(a^3+a^2+a+1\right)x^2 + \left(4a^3+8a^2+6a-11\right)x + \left(-3a^3+29a^2+11a-27\right).$$

The quotient of D_δ by $\operatorname{Aut} D_\delta$ is $\mathbb{P}^1$; the quotient map $\phi_\delta : D_\delta \to \mathbb{P}^1$ is defined over $\mathbb{Q}$ and factors through the map $D_\delta \to E_\pm$:



We are thus in the situation of elliptic Chabauty – by construction, any K-point of $E_\pm$ that is the image of a $\mathbb{Q}$-point of D_δ maps to $\mathbb{P}^1(\mathbb{Q})$ under ψ_δ, K has degree 4 and $E_\pm(K)$ has rank 2. Magma computes that the only K-rational points of E that map to $\mathbb{P}^1(\mathbb{Q})$ are the known ones coming from D_δ.

It takes a bit of work to compute explicitly the map $\psi_\delta : E_\pm \to \mathbb{P}^1$. The group H is not normal, so ψ_δ is not given by the quotient of a group of automorphisms. We proceed by brute force. We know the degree of ψ_δ and thus the general form of its equations (by Lemma 4.2). We construct points on D_δ over various number fields; we can map them on the one hand to $E_\pm$ and on the other hand to $\mathbb{P}^1$, giving a collection of pairs $(P \in E_\pm(\overline{K}), \psi_\delta(P))$. Sufficiently many such pairs will allow us to compute equations for ψ_δ.

See the transcript of computations for code verifying these claims. We find that there are six rational points on X_{619}. Two of these are cusps, two of these are CM points, corresponding to $j = 16581375$ (CM curves with discriminant -28), and two of these

correspond to $j = \frac{857985^3}{62^8}$. Three other curves in our list are isomorphic to X_{619}. One of these, X_{649} also has non-CM rational points corresponding to $j = \frac{919425^3}{496^4}$.

9.4 Analysis of X_{628}

The (probable) analytic rank of the Jacobian of X_{628} is 3, ruling out the possibility of a direct Chabauty argument. While it admits an étale double cover, the Prym variety associated to each twist has rank 1 and Chabauty on the double cover is thus possible but tedious to implement. Alternatively, each étale double cover maps to a rank 0 elliptic curve. This map is not explicit and would require a moderate amount of ad hoc work to exploit.

Instead, we exploit the nice model $y^4 = 4xz(x^2 - 2z^2)$ of this curve via the following direct argument. (This is equivalent to étale descent, but the simplicity of the model motivates a direct presentation.) An elementary argument shows that, for $xyz \neq 0$, there exist integers u, v, w such that either $x = \pm u^4, z = \pm 4v^4$, and $x^2 - 2z^2 = \pm w^4$, giving $u^8 - 32v^8 = \pm w^4$, or that $x = \pm 2u^4, z = \pm v^4$, and $x^2 - 2z^2 = \pm 2w^4$, giving $2u^8 - v^8 = \pm w^4$. It follows from ([14], Exercise 6.24, Proposition 6.5.4) that the only solution is to the latter equation with $u = v = w = 1$. It follows that the only points on $y^4 = 4xz(x^2 - 2z^2)$ are $(0 : 0 : 1)$, $(1 : 0 : 0)$, $(2 : -2 : 1)$ and $(2 : 2 : 1)$.

9.5 Analysis of X_{641} and X_{650}

Each of X_{641} and X_{650} have Jacobians of (probable) analytic rank 3, but admit various étale double covers. Each double cover has a twist with local points and such that the associated Prym variety has rank 1. This suggests a Chabauty argument via the Prym, but the details of such an implementation would be complicated. Instead we exploit the nice plane quartic models of these curves.

X_{641} has an affine model $(x^2 - 2y^2 - 2z^2)^2 = (y^2 - 2yz + 3z^2)(y^2 + z^2)$ and thus admits an étale double cover by the curve

$$\begin{aligned} D_\delta \colon y^2 - 2yz + 3z^2 &= \delta u^2 \\ x^2 - 2y^2 - 2z^2 &= \delta uv \\ y^2 + z^2 &= \delta v^2. \end{aligned}$$

The only twist with 2-adic points is $\delta = 1$. The quotient by the automorphism $[x : y : z : u : v] \mapsto [-x : y : z : -u : -v]$ is the genus 3 hyperelliptic curve $y^2 = -x^8 + 8x^6 - 20x^4 + 16x^2 - 2$. This curve is an unramified double cover of $H \colon y^2 = -x^5 + 8x^4 - 20x^3 + 16x^2 - 2x$. The Jacobian of H has rank 1, and Chabauty successfully determines the rational points on H; computing the preimages of these points on D allows us to conclude that only rational points on X_{641} are the known ones.

Similarly, X_{650} has a model $y^4 = (x^2 - 2xz - z^2)(x^2 + z^2)$ and thus admits an étale double cover by the curve

$$\begin{aligned} D_\delta \colon x^2 - 2xz - z^2 &= \delta u^2 \\ y^2 &= \delta uv \\ x^2 + z^2 &= \delta v^2 \end{aligned}$$

The only twist with 2-adic points is $\delta = 1$. This genus 5 curve has four automorphisms over $\mathbb{Q}$, and the quotient of D_1 by one of the involutions is the genus 3 hyperelliptic curve $y^2 = -x^8 + 2$, which maps to the genus 2 curve $H \colon y^2 = -x^5 + 2x$. The rank of the

Jacobian of H is 1, and Chabauty again proves that the only rational points on X_{650} are the known points.

10 Analysis of Rational Points - Genus 5 and 7

There are 20 genus 5 curves (at most 10 isomorphism classes) and 4 genus 7 curves. The genus 5 curves X_{686} and X_{689} are handled in an ad hoc manner by explicit étale descent. The remaining genus 5 curves and all of the genus 7 curves are handled by the modular double cover method (see Subsection 10.3) or are isomorphic to one of X_{686} or X_{689}.

10.1 Analysis of X_{689}

The curve X_{689} has a model

$$\begin{aligned} X_{672}\colon y^2 &= x^3 + x^2 - 3x + 1 \\ w^2 &= 2\left(y^2 + y(-x+1)\right)\left(x^2 - 2x - 1\right) \end{aligned}$$

The curve D_δ

$$\begin{aligned} y^2 &= x^3 + x^2 - 3x + 1 \\ \delta w_1^2 &= \left(x^2 - 2x - 1\right) \\ \delta w_2^2 &= 2\left(y^2 + y(-x+1)\right) \end{aligned}$$

is an étale double cover of X_{689}. (Magma computes that $g(D) = 9$, so this follows from Riemann-Hurwitz.) The cover is unramified outside of 2, so every rational point on X_{689} lifts to a rational point on D_δ for some $\delta \in \{\pm 1, \pm 2\}$. The curve D_δ maps to the curve H_δ given by

$$\begin{aligned} y^2 - \left(x^3 + x^2 - 3x + 1\right) &= 0 \\ \delta w_1^2 - \left(x^2 - 2x - 1\right) &= 0 \end{aligned}$$

which Magma computes is a genus 3 hyperelliptic curve. Each of these hyperelliptic curves has Jacobian of rank 1 or 2, with four visibile automorphisms. Taking the quotient by a non-hyperelliptic involution gives a genus 2 hyperelliptic curve, the Jacobians of which have rank at most 1; Chabauty applied to the genus 2 curves thus proves that the only rational points on X_{672} are the known points.

See the transcript of computations for Magma code verifying these claims.

10.2 Analysis of X_{686}

Similarly, the curve X_{686} has a model

$$\begin{aligned} X_{686}\colon y^2 &= x^3 + x^2 - 3x + 1 \\ w^2 &= 2\left(y^2 - y(-x+1)\right)\left(x^2 - 2x - 1\right) \end{aligned}$$

and étale double covers $D_\delta \to X_{686}$ from the curves

$$\begin{aligned} y^2 &= x^3 + x^2 - 3x + 1 \\ \delta w_1^2 &= x^2 - 2x - 1 \\ \delta w_2^2 &= 2\left(y^2 - y(-x+1)\right). \end{aligned}$$

The curve D_δ maps to the genus 3 hyperelliptic curve H_δ given by

$$\begin{aligned} y^2 - \left(x^3 + x^2 - 3x + 1\right) &= 0 \\ \delta w_1^2 - \left(x^2 - 2x - 1\right) &= 0. \end{aligned}$$

These are the same curves as in the analysis of X_{689}, and we conclude in the same way that the only rational points on X_{686} are the known points.

10.3 Non-explicit, modular double covers

The remaining genus 5 curves and the genus 7 curves are inaccessible via other methods and will be handled by the modular double cover method described in subsection 7.4. We describe this method in more detail here.

Let $S = \{1, 2, -1, -2\}$ and for $\delta \in S$ define χ_δ to be the Kronecker character associated to $\mathbb{Q}(\sqrt{\delta})$. Suppose that X is one of these 20 such curves, with corresponding subgroup H. In each case, we can find four index 2 subgroups K_δ with $\delta \in S$ so that for all $g \in K_\delta$,

$$g \in K_1 \text{ if and only if } \chi_\delta(\det g) = 1.$$

Moreover, if the genus of X is g, the genus of each K_δ is $2g - 1$, which implies that X_{K_δ}/X is étale.

Choose a modular function $h(z)$ for K_1 so that if m is an element of the non-identity coset for K_1 in H, then $h|m = -h$. A model for X_{K_1} is then given by $h^2 = r$, where $r \in \mathbb{Q}(X_H)$. Moreover, the condition on elements of K_δ implies that $\sqrt{\delta}h$ is fixed by the action of K_δ (recall the method of model computations in Section 4). This implies that the curves X_{K_δ} are the twists (by the elements of S) of K_1, and hence every rational point on X_H lifts to one of the X_{K_δ}. In each case, the X_{K_δ} maps to a curve X_n whose model we have computed that has finitely many rational points (namely a pointless conic, a pointless genus 1 curve, or an elliptic curve with rank zero).

Note that the group theory alone provides the properties we need for the curves X_{K_δ}, and we do not construct models for them.

Example 10.4. The curve X_{695} is a genus 5 curve that has two visible rational points corresponding to elliptic curves with j-invariant 54000. In this case, X_{K_1} and $X_{K_{-1}}$ map to the rank zero elliptic curve $X_{285} : y^2 = x^3 + x$ (whose two rational points map to $j = 54000$). The curves X_{K_2} and $X_{K_{-2}}$ map to X_{283}, a genus 1 curve with no 2-adic points.

See the transcript of computations for further details.

Appendix A: Proving the mod *N* representation is surjective

Given a Galois extension $K/\mathbb{Q}$ with Galois group G, [17] gives an algorithm that will allow one to determine, for a given unramified prime p, the Frobenius conjugacy class Frob_p. Applied to the case $K = \mathbb{Q}(E[N])$, and given initial knowledge that G is a subgroup of some particular H (e.g. E could arise from a rational point on X_H), this gives an algorithm to prove that $\mathrm{im}\rho_{E,N} = H$.

Remark A.1. When $H = S_n$ or $\mathrm{GL}_2(\mathbb{F}_\ell)$ this is well understood (e.g. in the latter case, if $\ell > 5$ and G contains three elements with particular properties then

$G = H$ [39]*Prop. 19). For subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$, [48] recently proved that if two subgroups H, K of $\mathrm{GL}_2(\mathbb{F}_\ell)$ have the same *signature*, defined to be

$$s_H := \{(\det A,\ \mathrm{tr}\, A,\ \mathrm{rank\ fix}\, A) : A \in H\},$$

then H and K are conjugate. (Note that the extra data of fix A is necessary to distinguish the trivial and order 2 subgroups of $\mathrm{GL}_2(\mathbb{F}_2)$. Already for $G \subset \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})$ with $\ell > 2$, the additional data of fix A does not suffice – for instance, the order ℓ subgroups generated by

$$\begin{bmatrix} 1-\ell & \ell \\ 0 & 1+\ell \end{bmatrix} \text{and} \begin{bmatrix} 1-\ell & -\ell \\ 0 & 1+\ell \end{bmatrix}$$

have the same signature).

Remark A.2. It is in principle completely straight-forward to provably determine the image of $\rho_{E,n}$. Indeed, Magma can compute, for any n, the corresponding division polynomial, and compute the Galois group of the corresponding field. In practice though, as the degree of $\mathbb{Q}(E[\,n]\,)$ grows, a direct computation of the Galois group using Magma's built in commands quickly becomes infeasible.

We now describe the algorithm. Suppose that K is the splitting field of

$$F(x) = \prod_{i=1}^{n} (x - a_i).$$

Given some fixed polynomial h and a conjugacy class $C \subseteq G$, construct the resolvent polynomial

$$\Gamma_C(X) = \prod_{\sigma \in C} \left(X - \sum_{i=1}^{n} h(a_i)\sigma(a_i) \right).$$

Theorem 5.3 of [17] states the following (specializing to extensions of $\mathbb{Q}$).

Theorem. Assume the notation above.

(1) For each conjugacy class $C \subseteq G$, $\Gamma_C(X)$ has coefficients in $\mathbb{Q}$.
(2) If p is a prime that does not divide the denominators of $F(x)$, $h(x)$ and the resolvents of Γ_C and $\Gamma_{C'}$ for different C and C', then

$$\mathrm{Frob}_p = C \iff \Gamma_C \left(\mathrm{Tr}_{\frac{\mathbb{F}_p[x]}{F(x)}/\mathbb{F}_p} (h(x)x^p) \right) \equiv 0 \pmod{p}.$$

We wish to apply this theorem in the case that $G = H$ and when the Galois group of $K/\mathbb{Q}$ may not necessarily be G. An examination of the proof shows that the theorem remains true even if $\mathrm{Gal}(K/\mathbb{Q})$ is a proper subgroup of G.

Our setup is the following. Suppose that $E/\mathbb{Q}$ is an elliptic curve with a model chosen that has integer coefficients. Suppose also that we know, a priori, that the image of the

mod N Galois representation is contained in $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The following algorithm gives a method to prove that the mod N image is equal to H. Define

$$s_1(N) = \begin{cases} 4 & \text{if } N = 2 \\ p \text{ if } N > 2 \text{ is a power of the prime } p \\ 1 & \text{otherwise,} \end{cases}$$

$$s_2(N) = \begin{cases} 8 & \text{if } N = 2 \\ 9 & \text{if } N = 3 \\ p \text{ if } N > 3 \text{ is a power of the prime } p \\ 1 & \text{otherwise.} \end{cases}$$

(1) We fix an isomorphism $\phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$ and pre-compute decimal expansions of $f(P) = s_1(N)x(P) + s_2(N)y(P)$ for all torsion points of P of order N on E. By Theorem VIII.7.1 of [43], these numbers are algebraic integers.

(2) The action of Galois on the numbers $s_1(N)x(P) + s_2(N)y(P)$ is given by some conjugate of H. We attempt to identify a unique conjugate of H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that gives this action. We do this by numerically computing

$$\sum_{k\in K} f(\phi(k(1,0)))f(\phi(k(0,1)))+f(\phi(k(1,0)))f(\phi(k(1,1)))+f(\phi(k(0,1)))f(\phi(k(1,1)))$$

for each conjugate K of H inside $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. If the image of the mod N representation is contained in K, then the sum above will be an integer.

(3) We compute the polynomial $F(x)$ with integer coefficients whose roots are the numbers $f(P) = s_1(N)x(P) + s_2(N)y(P)$. This polynomial is computed numerically. Knowing the size of the numbers $f(P)$, we verify that enough decimal precision is used to be able to round the coefficients of $F(x)$ to the nearest integer and obtain the correct result.

(4) We compute the resolvent polynomials for all of the conjugacy classes of H and check that these have no common factor. (In practice, we use $h(x) = x^3$ to construct these polynomials. We use a smaller decimal precision for the resolvent polynomials and again check that we can round the coefficients to the nearest integer to obtain the correct result).

(5) Using the resolvent polynomials, we compute the conjugacy class of $\rho_{E,N}(\mathrm{Frob}_p) \subseteq H$ for lots of different primes p.

(6) We enumerate the maximal subgroups of H and determine which conjugacy classes they intersect. We check to see if the conjugacy classes found in the previous step all lie in some proper maximal subgroup of H. If not, then the image of $\rho_{E,N}$ is equal to H.

Note that it is not possible for a maximal subgroup $M \subseteq H$ to intersect all of the conjugacy classes of H.

Example A.3. Let $E : y^2 = x^3 + x^2 - 28x + 48$. This elliptic curve has j-invariant 78608, which corresponds to a non-CM rational point on X_{556}, and hence the 2-adic image for E is contained in H_{556}, an index 96 subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ that contains $\Gamma(16)$. We must show that the 2-adic image equals H_{556}. Every maximal subgroup of H_{556} also contains $\Gamma(16)$, so it suffices to compute the image of the mod 16 Galois representation attached to E. To do this, we fix an isomorphism $E[16] \cong (\mathbb{Z}/16\mathbb{Z})^2$, and precompute decimal expansions

of $2x(P) + 2y(P)$ for all $P \in E[16]$, using 1000 digits of decimal precision. There are 24 conjugates of H_{556} in $\mathrm{GL}_2(\mathbb{Z}_2)$, and we find that the expression in step 2 above is an integer only for one of the conjugates of H_{556}.

The image of H_{556} under the map $\mathrm{GL}_2(\mathbb{Z}_2) \to \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z})$ has 46 conjugates classes, and we compute the polynomial $F(x)$ whose roots are the 192 numbers $2x(P) + 2y(P)$. Knowing the sizes of the roots, we can see that no coefficient of $F(x)$ could be larger than 10^{291}, and so 1000 digits of decimal precision is enough to correctly recover $F(x)$.

We then compute the resolvent polynomials for the 46 conjugacy classes (using 500 digits of decimal precision). Then, for each prime $p \leq 30000$, we compute $\mathrm{Tr}_{\frac{\mathbb{F}_p[x]}{(F(x))}/\mathbb{F}_p}(x^{p+3})$ and check which resolvent polynomial has this number as a root in $\mathbb{F}_p$. Using this, we can determine which conjugacy class is the image of Frob_p. We find that all 46 conjugacy classes are in the image of Frob_p for some p. (For example, the smallest prime p which splits completely in $\mathbb{Q}(E[16])$ is $p = 5441$.) As a consequence the image of the mod 16 Galois representation of E is H_{556}.

Acknowledgments

We thank Jeff Achter, Nils Bruin, Tim Dokchitser, Bjorn Poonen, William Stein, Michael Stoll, Drew Sutherland, and David Zywina for useful conversations and University of Wisconsin-Madison's Spring 2011 CURL (Collaborative undergraduate research Labs) students (Eugene Yoong, Collin Smith, Dylan Blanchard) for doing initial group theoretical computations. The second author is supported by an NSA Young Investigator grant. We would also like to thank anonymous referees for helpful comments and suggestions that have improved the paper.

Author details

[1] Department of Mathematics, Wake Forest University, Winston-Salem, NC 27109. [2] David Zureick-Brown, Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322 USA.

Received: 26 May 2015 Accepted: 29 June 2015
Published online: 07 October 2015

References

1. Arai, K: On uniform lower bound of the Galois images associated to elliptic curves. J. Théor. Nombres Bordeaux. **20**(1), 23–43 (2008). http://jtnb.cedram.org/item?id=JTNB_2008__20_1_23_0
2. Baran, B: A modular curve of level 9 and the class number one problem. J. Number Theory. **129**(3), 715–728 (2009). http://dx.doi.org/10.1016/j.jnt.2008.09.013
3. Baran, B: Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. J. Number Theory. **130**(12), 2753–2772 (2010). http://dx.doi.org/10.1016/j.jnt.2010.06.005
4. Baran, B: An exceptional isomorphism between modular curves of level 13. J. Number Theory. **145**, 273–300 (2014)
5. Bröker, R, Lauter, K, Sutherland, AV: Modular polynomials via isogeny volcanoes. Math. Comp. **81**(278), 1201–1231 (2012). http://dx.doi.org/10.1090/S0025-5718-2011-02508-1
6. Bilu, Y, Parent, P, Rebolledo, M: Rational points on $X_0^+(p^r)$ (2011). arXiv:1104.4641, Preprint
7. Bruin, N, Poonen, Bj, Stoll, M: Generalized explicit descent and its application to curves of genus, 3 (2012). Preprint
8. Bruin, N: Chabauty methods using elliptic curves. J. Reine Angew. Math. **562**, 27–49 (2003)
9. Bruin, N: Some ternary Diophantine equations of signature (*n*,*n*,2). In: Discovering mathematics with Magma, Algorithms Comput. Math. vol. 19, pp. 63–91. Springer, Berlin, (2006). http://dx.doi.org/10.1007/978-3-540-37634-7_3
10. Bruin, N: The arithmetic of Prym varieties in genus 3. Compos. Math. **144**(2), 317–338 (2008). http://dx.doi.org/10.1112/S0010437X07003314
11. Bruin, N, Stoll, M: Deciding existence of rational points on curves: an experiment, Experiment. Math. **17**(2), 181–189 (2008). http://projecteuclid.org/getRecord?id=euclid.em/1227118970
12. Coombes, KR, Grant, DR: On heterogeneous spaces. J. London Math. Soc. (2). **40**(3), 385–397 (1989). http://dx.doi.org/10.1112/jlms/s2-40.3.385
13. Chen, I: On Siegel's modular curve of level 5 and the class number one problem. J. Number Theory. **74**(2), 278–297 (1999). http://dx.doi.org/10.1006/jnth.1998.2320
14. Cohen, H: Number theory. Vol. I. Tools and Diophantine equations. Graduate Texts in Mathematics, Vol. 239. Springer, New York (2007)
15. Cummins, CJ, Pauli, S: Congruence subgroups of PSL$(2,\mathbb{Z})$ of genus less than or equal to 24. Experiment. Math. **12**(2), 243–255 (2003). http://projecteuclid.org/getRecord?id=euclid.em/1067634734
16. Dokchitser, T, Dokchitser, V: Surjectivity of mod 2^n representations of elliptic curves. Math. Z. **272**(3-4), 961–964 (2012). http://dx.doi.org/10.1007/s00209-011-0967-7
17. Dokchitser, T, Dokchitser, V: Identifying Frobenius elements in Galois groups. Algebra Number Theory. **7**(6), 1325–1352 (2013). http://dx.doi.org/10.2140/ant.2013.7.1325

18. Deligne, P, Rapoport, M: Les schémas de modules de courbes elliptiques. In: Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math, pp. 143–316. Springer, Berlin, (1973)
19. Diamond, F, Shurman, J: A first course in modular forms: Graduate Texts in Mathematics, Vol. 228. Springer-Verlag, New York (2005)
20. Elkies, ND: Elliptic curves with 3-adic galois representation surjective mod 3 but not mod 9 (2006). Preprint
21. Flynn, EV, Wetherell, JL: Covering collections and a challenge problem of Serre. Acta Arith. **98**(2), 197–205 (2001). http://dx.doi.org/10.4064/aa98-2-9
22. González-Jiménez, E, González, J: Modular curves of genus 2, Vol. 72 (2003). http://dx.doi.org/10.1090/S0025-5718-02-01458-8
23. González-Jiménez, E, Lozano-Robledo, Á: Elliptic curves with abelian division fields. Preprint
24. Hecke, E: Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik. Abh. Math. Sem. Univ. Hamburg. **5**(1), 199–224 (1927). http://dx.doi.org/10.1007/BF02952521
25. Heegner, K: Diophantische Analysis und Modulfunktionen. Math. Z. **56**, 227–253 (1952)
26. Jones, JW: Number fields unramified away from 2. J. Number Theory. **130**(6), 1282–1291 (2010). http://dx.doi.org/10.1016/j.jnt.2010.02.005
27. Jones, R, Rouse, J: Galois theory of iterated endomorphisms. Proc. Lond. Math. Soc. (3). **100**(3), 763–794 (2010). http://dx.doi.org/10.1112/plms/pdp051. Appendix A by Jeffrey D. Achter
28. Kenku, MA: A note on the integral points of a modular curve of level 7. Mathematika. **32**(1), 45–48 (1985). http://dx.doi.org/10.1112/S0025579300010846
29. Knapp, AW: Elliptic curves. Mathematical Notes, Vol. 40. Princeton University Press, Princeton, NJ (1992)
30. Mazur, B: Rational points on modular curves. In: Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 107–148. Springer, Berlin, (1977)
31. Mazur, B: Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. **44**(2), 129–162 (1978)
32. McMurdy, K: Explicit equations for $X_{0(N)}$. http://phobos.ramapo.edu/~kmcmurdy/research/Models/index.html
33. Momose, F: Rational points on the modular curves $X_{\mathrm{split}(p)}$. Compositio Math. **52**(1), 115–137 (1984). http://www.numdam.org/item?id=CM_1984__52_1_115_0
34. McCallum, W, Poonen, B: The method of Chabauty and Coleman. Soc. Math., France, Paris (2012)
35. Nishioka, K: The 2-adic representations attached to elliptic curves defined over Q whose points of order 2 are all Q-rational. J. Math. Soc. Japan. **35**(2), 191–219 (1983). http://dx.doi.org/10.2969/jmsj/03520191
36. Poonen, B: Computing rational points on curves. In: Number theory for the millennium, III (Urbana, IL, 2000), pp. 149–172. A K Peters, Natick, MA, (2002)
37. Poonen, B, Schaefer, EF: Explicit descent for Jacobians of cyclic covers of the projective line. J. Reine Angew. Math. **488**, 141–188 (1997)
38. Rouse, J, Zureick-Brown, D: Electronic transcript of computations for the paper 'Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois'. Available at, http://users.wfu.edu/rouseja/2adic/. (Data files and scripts will also be posted on arXiv)
39. Serre, J-P: Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**(4), 259–331 (1972)
40. Serre, J-P: Lectures on the Mordell-Weil theorem. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. With a foreword by Brown and Serre. 3rd ed. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig (1997). x+218 pp. ISBN: 3-528-28968-6 MR1757192(2000m:11049)
41. Shimura, G: Introduction to the arithmetic theory of automorphic functions. In: Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, (1971). Kanô Memorial Lectures, No. 1
42. Shimura, M: Defining equations of modular curves $X_{0(N)}$. Tokyo J. Math. **18**(2), 443–456 (1995). http://dx.doi.org/10.3836/tjm/1270043475.
43. Silverman, JH: The arithmetic of elliptic curves, Second edition, Graduate Texts in Mathematics, Vol. 106. Springer, Dordrecht (2009)
44. Skorobogatov, A: Torsors and rational points, Cambridge Tracts in Mathematics, Vol. 144. Cambridge University Press, Cambridge (2001). http://dx.doi.org.ezproxy.library.wisc.edu/10.1017/CBO9780511549588
45. Schoof, R, Tzanakis, N: Integral points of a modular curve of level 11. Acta Arith. **152**(1), 39–49 (2012). http://dx.doi.org/10.4064/aa152-1-4
46. Stoll, M: Implementing 2-descent for Jacobians of hyperelliptic curves. Acta Arith. **98**(3), 245–277 (2001). http://dx.doi.org/10.4064/aa98-3-4
47. Sutherland, AV: Constructing elliptic curves over finite fields with prescribed torsion. Math. Comp. **81**(278), 1131–1147 (2012). http://dx.doi.org/10.1090/S0025-5718-2011-02538-X
48. Sutherland, AV: Computing images of Galois representations attached to elliptic curves (2015). arXiv:1504.07618, Preprint
49. Sutherland, A: Defining equations for $X_1(N)$. http://math.mit.edu/~drew/X1_altcurves.html
50. Stoll, M, van Luijk, R: Explicit Selmer groups for cyclic covers of $\mathbb{P}^1$. Acta Arith. **159**(2), 133–148 (2013). http://dx.doi.org/10.4064/aa159-2-4
51. Sutherland, A, Zywina, D: Modular curves of genus zero and prime-power level. in preparation
52. Wetherell, JL: Bounding the number of rational points on certain curves of high rank. ProQuest LLC, Ann Arbor, MI (1997). http://search.proquest.com/docview/304343505. Thesis (Ph.D.)–University of California, Berkeley
53. Wilson, JS: Profinite groups. London Mathematical Society Monographs. New Series. The Clarendon Press Oxford University Press, New York (1998)
54. Zywina, D: On the surjectivity of mod l representations associated to elliptic curves (2011). Preprint